POLITECNICO DI MILANO

Facoltà di Ingegneria dei Sistemi

Corso di Laurea Magistrale in Ingegneria Gestionale

Anno accademico 2010/2011

Tesi di laurea magistrale:

IL RUOLO DEGLI STRUMENTI CULTURALI PER LA SICUREZZA DELLE ILU SUPPLY CHAIN

Relatore:

Prof. Margherita Pero

Lavoro di:

Quadri Alessia matr. 751847

Savoia Daniele matr. 749984

Sodano Luigi matr. 755206

Ringraziamenti:

Il primo ringraziamento è per la nostra relatrice Prof. Margherita Pero che ci ha proposto questo lavoro di tesi, ma soprattutto ci ha dato la possibilità di scegliere, modificare, approfondire delle tematiche di nostro interesse e ci ha sempre fornito pieno supporto e disponibilità.

Un ringraziamento doveroso è per Walter Savoia che ci ha procurato molti contatti per poter effettuare le interviste in azienda tanto importanti per questo lavoro.
A questo proposito un grazie va a tutte le aziende e le persone che si sono rese diponibili per le interviste: Riccardo Ambrogio (Ambrogio), Alessandro Negri (BAS), Laura fortina (Ewals Intermodal), Gianfranco Brillante (Fercam), Sabrina Robba (Hoyer), Sergio Crespi (Hupac), Gian Luca Fossati (Interporto Rivalta Scrivia), Francesca Doria (Marenzana), Bruno Carbonin (MDB), Fabrizio Filippi (Sogemar), Davide Muzio (T.I.MO), Aldo Locurcio (Terminali Italia) e Giovanni Mazzali (VOTG).
Un ringraziamento particolare va inoltre all'Ing. Fulvio Quattroccolo per la sua disponibilità e il grosso aiuto che ci ha dato per capire al meglio il "mondo dell'intermodale".

Un altro ringraziamento di cuore è rivolto a (e scusate la scarsa modestia) noi stessi: Ale, Gigi e Savo. In questi mesi di assiduo lavoro siamo sempre rimasti uniti, ci siamo dati forza l'un l'altro facendoci anche (diciamo la verità a tutti) tante risate. Ci siamo impegnati veramente affinchè questa tesi risultasse un buon lavoro sacrificando (se di sacrificio si può parlare) giornate intere in quella calda aula sotto la Nave a scrivere, riguardare (a volte anche troppo) e correggere ogni singola parola che troverete scritta da qui in avanti.

In ultimo, ma assolutamente non per importanza, ringraziamo di cuore i nostri familiari che ci hanno sostenuto economicamente e moralmente in questi 5 anni, le nostre dolci metà con le quali abbiamo condiviso le delusioni ma soprattutto le gioie (come quella enorme che esploderà il 21 dicembre 2011), tutti i nostri compagni di corso con cui abbiamo vissuto 5 anni bellissimi che non dimenticheremo mai e i nostri più cari amici che hanno sempre tenuto alto il nostro morale e ci hanno permesso di affrontare questi anni nel miglior modo possibile…. GRAZIE!

Indice

Indice delle figure

Indice delle tabelle

Executive summary

Ambito di ricerca[1]

Il nostro lavoro di Tesi si focalizza sulla sicurezza all'interno delle ILU supply chain. Con il termine ILU supply chain, intendiamo l'insieme di organizzazioni e attori che interagiscono tra di loro per portare dall'origine a destino il flusso di ILU (Intermodal Load Unit), ossia container, casse mobili e semirimorchi (IMCOSEC, 2010).

All'interno delle ILU supply chain il nostro focus è rivolto al trasporto intermodale strada-ferrovia, in particolare quello combinato che prevede la parte più consistente del trasporto effettuata su rotaia, mentre il primo e l'ultimo miglio effettuati su strada. I benefici caratteristici di questo nuovo approccio al trasporto sono da ricercare in prestazioni sociali (riduzione del traffico su strada), di sicurezza (utilizzato soprattutto per prodotti chimici pericolosi), energetiche (minor dispendio di energia) e di sostenibilità ambientale (riduzione di inquinanti atmosferici). Riconoscendo questi vantaggi, che esulano da un'analisi prettamente economica, l'Unione Europea ha effettuato svariati studi e intrapreso una serie di programmi in favore del trasporto intermodale. L'obiettivo di questi programmi è il bilanciamento nell'utilizzo delle diverse modalità di trasporto (strada, ferrovia, mare, vie navigabili interne, aereo); ad oggi il sistema di trasporto europeo è fortemente sbilanciato verso il trasporto su strada e in generale verso l'utilizzo di mezzi non sostenibili dal punto di vista ambientale ed energetico. Passando alla situazione italiana, allo stato attuale, le maggiori criticità che ostacolano lo sviluppo del trasporto intermodale sono di:

- natura infrastrutturale, inerenti sia l'assenza di interconnessioni fra le reti sia le differenze nella sagoma limite all'interno della rete ferroviaria;
- natura gestionale, legata alle caratteristiche intrinseche del trasporto intermodale. Coesistono infatti numerosi attori che svolgono operazioni diverse e non sempre hanno piena visibilità l'uno sull'altro; oltretutto il trasporto intermodale è meno flessibile di quello stradale e complica l'attività di ricerca di carichi per la tratta di ritorno;

[1] Scritto in collaborazione con l'Ing. Fulvio Quattroccolo, fondatore e gestore del sito web www.intermodale24-rail.net

- natura giuridica, riguardante in modo particolare il differente stato di attuazione delle direttive europee come quella sulla liberalizzazione del mercato ferroviario della trazione: gli ex-monopolisti (in Italia Trenitalia Cargo) sono i soli ad avere i certificati di sicurezza su tutta la rete, quindi di fatto su alcune tratte hanno ancora il monopolio; questo impedisce lo sviluppo di una reale concorrenza con effetto sull'efficienza nei trasporti e sui prezzi richiesti;
- assenza di una chiara divisione dei ruoli; in particolare si fa riferimento al ruolo dominante di alcune imprese che ricoprono contemporaneamente più ruoli e hanno partecipazioni in loro competitor, loro fornitori e loro clienti. Questa situazione potrebbe comportare interferenze sull'operatività quotidiana (favoreggiamento della partecipata) limitando di fatto lo sviluppo del trasporto intermodale.

Il trasporto intermodale strada-ferrovia può essere classificato secondo diverse dimensioni come la tipologia di ILU trasportata (container, casse mobili o semirimorchi), il sistema di trasporto (accompagnato o non accompagnato) o la tipologia di treno adottata (treno completo tra cui sistemi diretti, shuttle e gateway oppure treno a carico singolo). I ruoli atomici all'interno della filiera intermodale, individuati nel corso delle interviste, sono schematizzati in Figura 1.

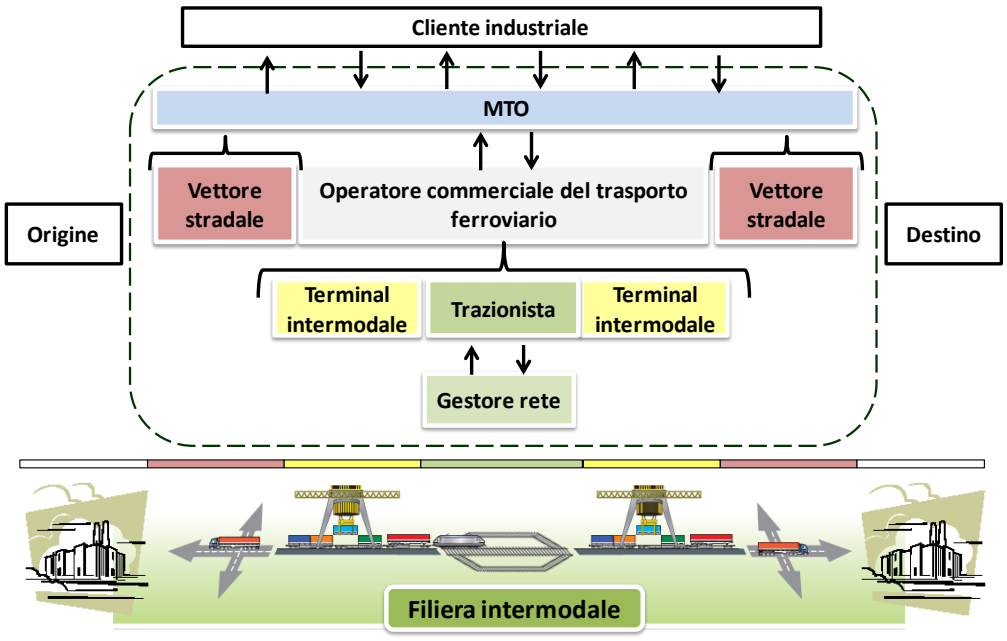


Figura 1: Classificazione dei vari attori della filiera intermodale strada-ferrovia

Analisi della letteratura

Per quanto riguarda il termine sicurezza, invece, abbiamo inizialmente preso in considerazione tutte le sue possibili accezioni. Dalla letteratura risulta che non esiste un significato univoco del concetto di sicurezza in quanto il termine italiano comprende due accezioni completamente diverse che vengono meglio espresse dai termini inglesi *security* e *safety*. Il primo corrisponde alla sicurezza del patrimonio tangibile e intangibile di un sistema[2], mentre il secondo riguarda la sicurezza delle persone, intesa come loro incolumità. Oltretutto la sicurezza può essere intesa in diversi modi anche in base all'approccio con cui essa viene analizzata che può essere di tipo normativo, manageriale, pratico, sociologico, organizzativo, tecnico, ingegneristico etc. In particolare ci siamo occupati della sicurezza del sistema di trasporto intermodale, quindi intesa come security, secondo l'approccio manageriale, organizzativo, sociologico e solo marginalmente tecnico.

Anche le organizzazioni hanno appreso il concetto di sicurezza secondo sfumature diverse. Le prime ricerche si sono incentrate su tematiche sociologiche e psicologiche, focalizzandosi sull'incolumità e il benessere delle persone. La preoccupazione di mettere al sicuro i propri beni durante il trasporto è emersa invece in letteratura soprattutto negli ultimi anni, con l'introduzione del concetto di Supply Chain Security (SCS).

Con SCS si intende un approccio che prevede l'applicazione di programmi, sistemi, procedure, tecnologie e soluzioni per affrontare le minacce a cui sono soggette le supply chain con l'obiettivo di migliorarne la sicurezza (Donner e Kruk, 2009; Closs e McGarrell, 2004; Burmeisters e Solovjovs, 2009).

A partire dal 11 settembre 2001 si è diffusa maggior consapevolezza tra le aziende sulle tematiche di sicurezza ed è iniziato il processo di cambiamento dell'approccio di SCS. In Figura 2 sono riassunti i principali cambiamenti, in parte ancora in corso.

[2] www.businessdictionary.com

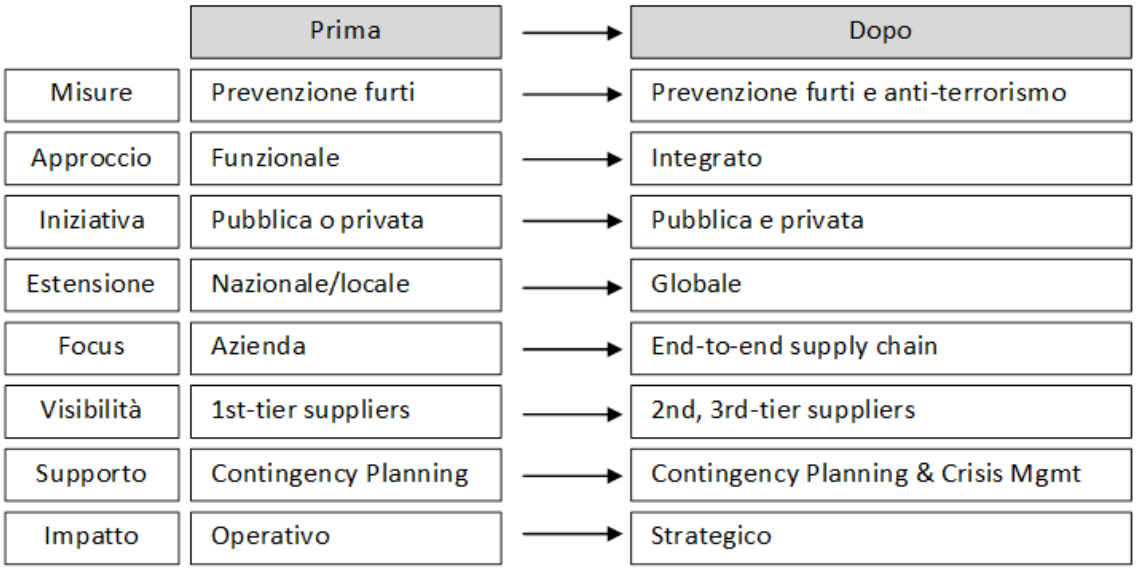


Figura 2: Modello per il cambiamento dei requisiti della Supply Chain Security

Le organizzazioni collocano le pratiche di SCS all'interno del sistema di Risk Management. Questo denota quanto sia importante effettuare un'accurata analisi dei rischi che le supply chain corrono, attraverso cui è possibile capire le strategie di sicurezza da applicare per ridurre le vulnerabilità. In riferimento alla matrice di vulnerabilità, con cui è possibile classificare ogni fonte di rischio in funzione della probabilità di accadimento e della severità delle conseguenze, risulta che per ridurre la vulnerabilità è possibile agire su entrambe le variabili. Queste determinano la prestazione di sicurezza, che può essere dettagliata in termini di sicurezza preventiva, ossia "*la capacità di un'impresa di monitorare e prevenire possibili fattori di destabilizzazione delle sue attività"* e di resilienza, ossia "*la capacità di un'impresa che ha subito una disruption di ripristinare le normali attività"* (Nassimbeni, 2009).

In Figura 3 si osserva che le strategie di SCS variano in base ai differenti rischi della supply chain e alle condizioni di contesto.

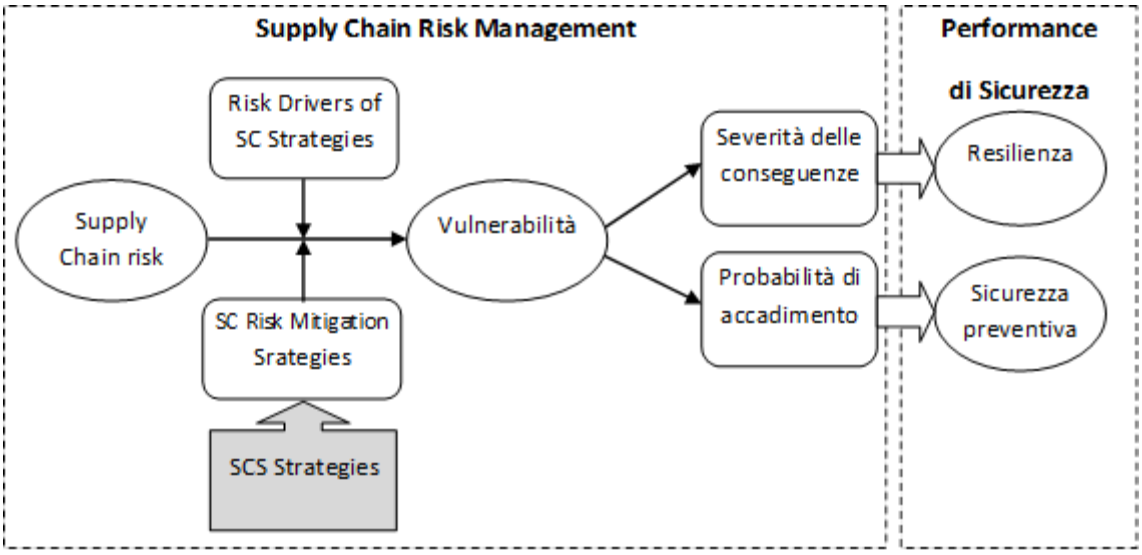


Figura 3: Supply chain risk management e performance di sicurezza

Tendenze recenti dimostrano come le organizzazioni abbiano rivolto una maggiore attenzione verso quei rischi derivanti da minacce intenzionali con conseguente focalizzazione sulle strategie che ne abbassano la probabilità di accadimento.

Dal punto di vista delle prestazioni organizzative di filiera, le strategie di SCS possono impattare anche su altre performance organizzative infatti hanno: un impatto diretto (e indiretto tramite la trasparenza) sulla sicurezza e sull'efficienza, indiretto sull'efficacia (tramite una maggiore sicurezza), e allo stesso tempo generano dei trade-off tra prestazioni di efficienza e sicurezza, come rappresentato in Figura 4.

In riferimento al trade-off efficienza-sicurezza, Willis e Ortiz (2004) hanno osservato che *"se si lavora sotto le "condizioni operative normali" si potrebbero avere effetti addirittura negativi"*; Sheffi (2001) e Nassimbeni (2009) individuano nel dettaglio alcune strategie di SCS che possono portare ad un peggioramento dell'efficienza, e al contrario, strategie di supply chain efficienti che possono portare a un peggioramento della sicurezza.

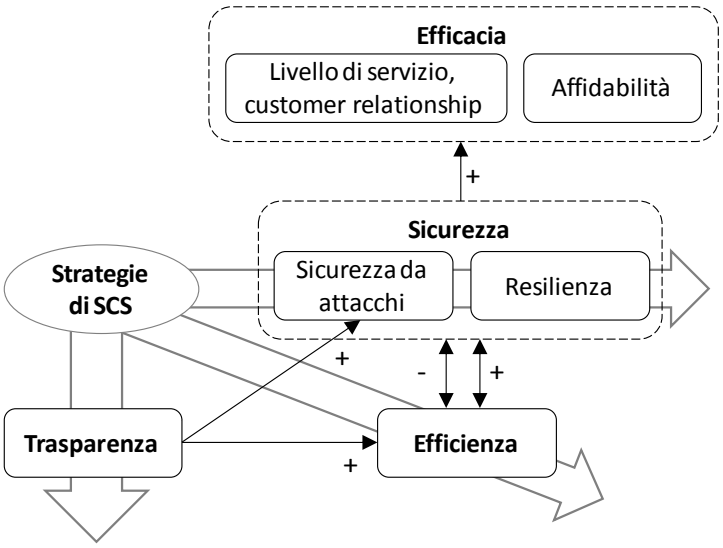


Figura 4: Mappa delle relazioni tra prestazioni organizzative

Dall'analisi delle relazioni tra SCS e prestazioni è emerso che i motivi che ostacolano la diffusione dell'approccio di SCS sono l'assenza di ricerche quantitative che dimostrino gli impatti positivi verso entrambe le prestazioni di efficienza ed efficacia, il trade-off tra le prestazioni di sicurezza ed efficienza, oltre alla mancanza di una corretta comunicazione delle pratiche di sicurezza e dei benefici ottenibili all'interno della supply chain.

L'approccio di SCS è stato successivamente declinato al nostro ambito di interesse, quello della filiera del trasporto intermodale, definita in letteratura da alcuni autori "container supply chain", o più in generale "ILU supply chain".

La globalizzazione delle aziende spiega la necessità da parte delle autorità governative e delle organizzazioni private di focalizzarsi sulla sicurezza della ILU supply chain. L'importanza di mettere al sicuro i flussi di container deriva dagli enormi rischi che corre il trasporto intermodale: infatti, più volte i container sono stati veicolo per il trasporto illegale di armi a distruzione di massa o per il trasporto clandestino di terroristi, oltre ad essere soggetti a furti e manipolazioni di ogni genere (Sarathy, 2005).

In particolare la ILU supply chain è esposta a vulnerabilità in corrispondenza di tutti gli elementi che la compongono: stabilimenti produttivi, unità di carico, fornitori, partner e organizzatori del trasporto, strutture logistiche, persone e informazioni (Sarathy, 2005, 2006).

Ulteriori difficoltà sono legate all'adozione di un approccio di SCS integrato in tutta la filiera che, insieme alla mancanza di una cultura di risk management, non permette di avere ben chiari tutti i rischi che le supply chain corrono, facendo quindi mancare il

presupposto fondamentale per la riduzione della vulnerabilità (Williams et al., 2008; IMCOSEC, 2010).

Con l'aumento dell'importanza riservata alle tematiche di SCS le autorità governative e le aziende hanno proposto dei programmi per la messa in sicurezza della catena di fornitura. Rispetto al focus tradizionale, questi nuovi programmi considerano la supply chain nella sua totalità, proponendo un approccio di collaborazione tra aziende e con le autorità governative (Donner e Kruk, 2009). In Tabella 1 sono riassunti i principali programmi ad applicazione volontaria promossi negli ultimi anni.

Tabella 1: Classificazione dei programmi volontari di sicurezza

Nome/anno di inizio	Paese di origine dell'istituto	Modalità	Partecipanti/ stato	Categoria	Obiettivo
TAPA, 1997	US	Trasporto su gomma	207 membri	Privata volontaria	Report incidenti criminali/identificazione soluzioni/condivisione informazioni
C-TPAT, 2001	US	Tutte	6375 certificazioni e 3916 aziende approvate	Governativa volontaria	Supply chain security
CSI, 2002	US	Trasporto via mare	58 porti	Governativa volontaria	Supply chain security
WCO SAFE FoS, 2005	WCO	Tutte	156 Stati membri	Internazionale volontaria	Standard per la supply chain security e per l'agevolazione del commercio
ISO 28000, 2005	Comitato tecnico ISO	Tutte	157 Paesi membri	Internazionale volontaria	Supply chain security
EU-AEO, 2008	Commissione Europea	Tutte	192 aziende	Governativa volontaria	Supply chain security e agevolazione del commercio

I nuovi approcci alla sicurezza si concentrano sulla security e hanno l'obiettivo di diffondere standard internazionali, di promuovere la diffusione e la condivisone di informazioni tra aziende e con le autorità governative, di sviluppare efficaci sistemi di gestione aziendale della sicurezza e di sviluppare dei processi che consentano una gestione integrata della filiera (Gutierrez e Hintsa, 2006). Dall'analisi dei principali programmi internazionali e della letteratura inerente alle pratiche di SCS, abbiamo ricavato la classificazione degli strumenti di sicurezza rappresentata in Figura 5.

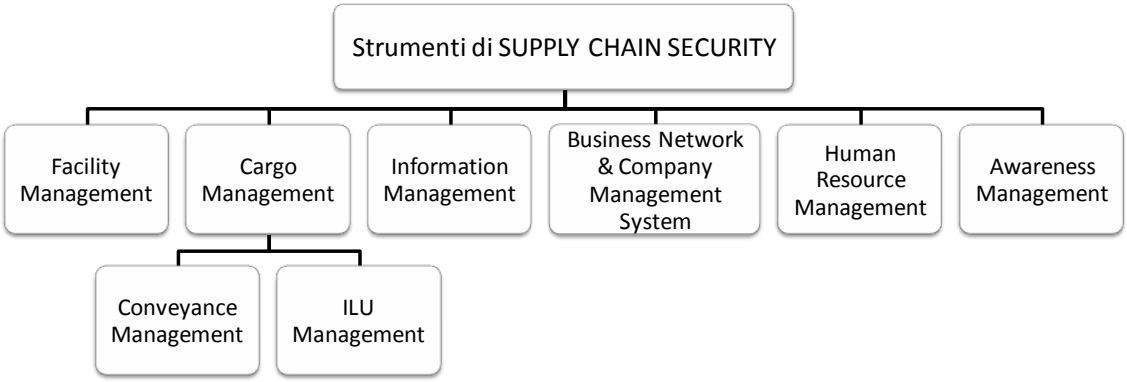


Figura 5: Classificazione ambiti SCS

La categoria "Facility Management" comprende tutti gli strumenti che consentono la messa in sicurezza delle strutture adibite all'immagazzinamento e alla gestione delle ILU; si passa da strumenti che in fase di progettazione consentono di abbassare i rischi della struttura a sistemi di difesa fisica fino a tecnologie per il monitoraggio e il controllo d'accesso. Gli strumenti di "Cargo Management" garantiscono invece la sicurezza del cargo durante tutti gli step del trasporto: in questa categoria si possono distinguere gli strumenti associati al mezzo di trasporto ("Conveyance Management") da quelli che assicurano la sicurezza della ILU rispetto a minacce intenzionali ("ILU Management"). Della prima categoria fanno parte la pianificazione delle ispezioni durante il trasporto, le soluzioni per il tracking e la gestione della rotta del cargo. Della seconda fanno parte le tecniche e le tecnologie per ispezionare le ILU e le soluzioni che vogliono impedirne la compromissione dell'integrità, di natura sia tecnologica che processuale/organizzativa. Gli strumenti di "Information Management" consentono di sfruttare le informazioni disponibili come mezzo per individuare anomalie, prevenire lacune di sicurezza e proteggere i dati critici del business. Si tratta di strumenti che permettono alle aziende di costruire un database informativo di qualità e di adottare pratiche per la salvaguardia delle informazioni e per la gestione della conoscenza in azienda. Gli strumenti della categoria "Business Network & Company Management System" consentono di rendere sicuro il sistema di gestione aziendale. Si tratta di strumenti che consentono la progettazione e l'implementazione di un sistema corporate di gestione della sicurezza e di progettare un sistema logistico flessibile e resiliente. In ottica di filiera, gli strumenti consentono la valutazione dei SC partner e l'instaurazione di relazioni collaborative con aziende ed enti governativi. Della categoria "Human Resource Management" fanno parte gli strumenti che si occupano di assicurare l'affidabilità delle persone che entrano in contatto con la ILU agendo sui processi di

selezione e di fine rapporto, sull'organizzazione dei ruoli e delle responsabilità di sicurezza in azienda. Nella categoria "Awarness Management" rientrano infine gli strumenti che garantiscono la consapevolezza sulla sicurezza del personale che entra in contatto con la ILU. Si tratta di iniziative per la formazione ed educazione del personale e per lo sviluppo della consapevolezza sulle tematiche di sicurezza in azienda e verso partner di filiera.

Disegno di ricerca

L'analisi della letteratura sulla SCS ci ha consentito di individuare nelle categorie di Information Management, Human Resource Management e Awareness Management gli strumenti meno approfonditi e sviluppati. Tali categorie hanno in comune la caratteristica di non essere strettamente legate a precisi processi o punti all'interno della supply chain, bensì sono legate al fattore umano. Abbiamo definito questi strumenti "culturali" perché agiscono su valori, motivazioni, atteggiamenti e comportamenti degli individui all'interno dell'organizzazione. Considerato lo scarso approfondimento di questi strumenti in letteratura, la loro trasversalità e l'importanza del fattore umano in relazione alla sicurezza (Lacey, 2010), abbiamo così deciso di focalizzare la nostra ricerca su di essi. Per definire al meglio il nostro disegno di ricerca abbiamo ritenuto opportuno definire il concetto di cultura organizzativa e capire la sua applicazione nelle organizzazioni in relazione alle tematiche di sicurezza. Alcuni autori hanno messo in luce la recente diffusione tra le organizzazioni del concetto di Supply Chain Security Culture (Benson, 2005; Williams et al., 2008); e di Supply Chain Security Orientation (Autry e Bobbitt, 2008; Williams et al., 2008). La loro diffusione deriva dalla combinazione di vari fattori quali il crescente focus verso le tematiche di SCS da parte delle autorità governative e le organizzazioni private, l'importanza del ruolo che le tematiche culturali ricoprono nell'influenza di obiettivi strategici, tattici e operativi delle aziende e la maggior consapevolezza che le persone di un'organizzazione e le organizzazioni stesse sono i principali responsabili della generazione di disruption, ma anche il mezzo per evitarle e porre loro rimedio (Lacey, 2010).

Sulla base di queste considerazioni, abbiamo deciso di studiare il ruolo degli strumenti di tipo culturale nello sviluppo della sicurezza delle ILU supply chain; abbiamo quindi delineato il nostro perimetro di indagine attraverso la definizione di 5 domande di ricerca:

1. Quali strumenti culturali sono adottati nelle aziende del settore intermodale?
2. Qual è l'impatto che l'applicazione di ogni strumento ha sulla prestazione di sicurezza?
3. Quali fattori di contesto spiegano l'adozione degli strumenti culturali?
4. I fattori di contesto spiegano anche gli impatti degli strumenti sulle prestazioni?
5. Quali sono i fattori causa più importanti nel determinare una cattiva prestazione di sicurezza? Sono diversi in funzione dei fattori di contesto?

Se in risposta alla domanda n° 1 sarebbe bastato effettuare delle interviste sul campo e riportarne i risultati, per rispondere alle altre domande è stato necessario costruire il modello teorico rappresentato in Figura 6, composto da quattro componenti correlate tra di loro.

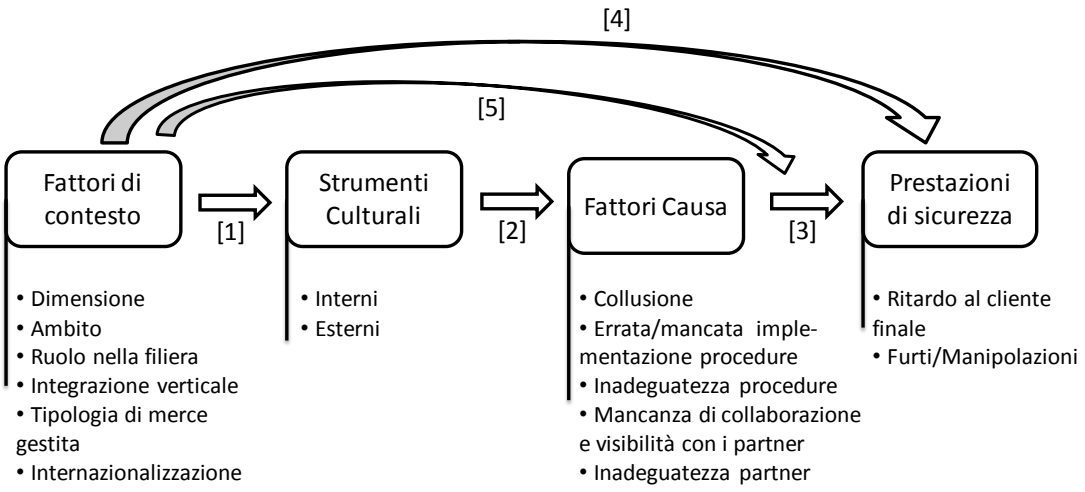


Figura 6: Modello teorico

La relazione [1] in Figura 6 presuppone l'esistenza di alcuni fattori di contesto discriminanti nell'utilizzo di un particolare strumento culturale (in risposta alla domanda di ricerca n° 3); la [2] indica il possibile impatto del singolo strumento culturale su uno specifico fattore causa, che a sua volta incide sulla prestazione di sicurezza finale [3] (la relazione [3] esprime cioè l'importanza relativa dei fattori causa per la prestazione di sicurezza e risponde alla prima parte della domanda di ricerca n°5). Le restanti relazioni suppongono invece che gli impatti degli strumenti [4] e dei fattori causa [5] sulle prestazioni di sicurezza possano variare in base ai fattori di contesto, in risposta rispettivamente alla domanda di ricerca n° 4 e 5. Per ricavare invece la risposta alla domanda di ricerca n° 2 basterà combinare le relazioni [2] e [3] e capire dunque l'impatto che ogni singolo strumento ha sulla sicurezza. I fattori di contesto

schematizzati in Figura 6 sono variabili che permettono di distinguere il profilo di un'azienda e si dividono in dimensione (grande, piccola), ambito (strada, ferrovia, entrambe), ruolo nella filiera intermodale (MTO, vettore stradale, gestore del terminal, operatore commerciale del trasporto ferroviario), integrazione verticale (alta, bassa), tipologia di merce trasportata (pericolosa, appetibile, altro) e internazionalizzazione (estesa su scala internazionale, solo Italia).

Passando agli strumenti culturali presi in considerazione dal modello in Figura 6 abbiamo riscontrato come, dall'analisi letteraria riferita alla SCSC, nessun autore abbia mai classificato questa tipologia di strumenti. Abbiamo dunque proposto una classificazione basata su quattro approcci alla security culture, riportata in Figura 7.

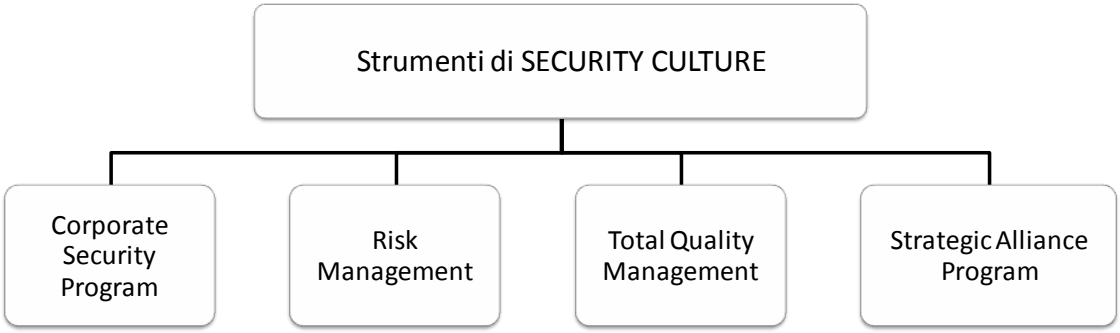


Figura 7: Classificazione degli approcci alla security culture

Nella Tabella 2 è riportato il dettaglio degli strumenti di SCSC individuati.

Tabella 2: strumenti di SCSC

CORPORATE SECURITY PROGRAM	Integrità, lealtà dei dipendenti	investigazione sul passato e colloqui con potenziali dipendenti e terze parti
		programmi di lealtà/fedeltà dei dipendenti
		HR policy
		span of control
	Competenza dei dipendenti sulle tematiche di sicurezza	coinvolgimento esperti esterni
		training dipendenti
		Team work
	Consapevolezza interna sulla sicurezza	assegnazione responsabilità di sicurezza al personale
		sistema di incentivazione e feedback sulla sicurezza
		Punizioni
		programmi di cambiamento organizzativo
		socializzazione informale
		comunicazione interna
		funzione/posizione dedicata alla security (CSO)
	Aspetti soft	simbolismo
		motto
		codice di condotta
RISK MANAGEMENT	Business continuity planning	training dipendenti
		empowerment dei dipendenti
		piani d'azione
	Segnalare incidenti e debolezze	analisi della natura e delle cause degli incidenti (anche minori)
		"Swiss Cheese" model
		monitoraggio dei "near misses"
	Valutazione della conformità di sicurezza	strumenti preventivi di sicurezza basati sull'esperienza reale
		certificazioni
TOTAL QUALITY MANAGEMENT	Partnership	norme di cooperazione
		relazioni di lungo termine
		condivisione di rischi, premi e responsabilità
		sviluppo della fiducia
	Collaborazione tra dipendenti	condivisione di rischi, premi e responsabilità
		teamwork
	Forza lavoro multidisciplinare	interazione cross-funzionale
		assunzione di persone con specifiche competenze
		training dei dipendenti
	Continuous improvement	funzione/posizione dedicata alla security (CSO)
		supporto del top management
		controllo dei processi esistenti
		empowerment dei dipendenti
	Focus sul cliente	-
	Knowledge management	apprendimento inter-aziendale
		istituzionalizzazione della conoscenza
STRATEGIC ALLIANCE PROGRAM	Sviluppo della consapevolezza sulla sicurezza con i miei partner	apprendimento inter-aziendale
		contratti con specifici requisiti di sicurezza
		educazione dei partner
	Riduzione delle differenze di cultura tra azienda e partner	sviluppo della fiducia
		comunicazione esterna
		hibridal cultural interface (HCI)
		socializzazione informale
	Partnership	norme di cooperazione
		relazioni di lungo termine
		Condivisone dei rischi, premi e responsabilità
		sviluppo della fiducia

L'approccio "Corporate Security Program" porta alla definizione di un piano strutturato per lo sviluppo e la diffusione di una cultura della sicurezza in azienda. Gli strumenti che lo costituiscono sono di tipo intra-aziendale e si dividono in programmi di

"**Integrità e lealtà dei dipendenti**" che servono per la selezione e l'affiliazione del personale, "**Competenza dei dipendenti sulle tematiche di sicurezza**" e "**Consapevolezza interna sulla sicurezza**" che agiscono sull'educazione, la formazione e la diffusione delle tematiche di security e gli "**Aspetti soft**" che hanno l'intento di creare una cultura organizzativa capace di influenzare le pratiche di lavoro quotidiano, agendo sulle filosofie, le ideologie, i valori e le aspettative delle persone. Nell'approccio di "Risk Management" sono presenti gli strumenti di stampo culturale che concorrono alla gestione dei rischi e delle vulnerabilità aziendali. Costituiscono questo approccio gli strumenti di "**Business continuity planning**" che descrivono il modo con cui un'organizzazione può far tornare operative le sue funzioni critiche a seguito di una disruption, quelli di "**Segnalazione di incidenti e debolezze**" per l'analisi delle cause degli incidenti/near misses occorsi e quelli di "**Valutazione della conformità di sicurezza**" per il controllo della conformità rispetto a requisiti di sicurezza (prevalentemente riconducibili ai principali programmi di sicurezza volontari). L'approccio di "Total Quality Management" si focalizza sugli strumenti tradizionalmente classificati come "soft TQM". Fanno parte di questo approccio gli strumenti inter-aziendali per l'instaurazione e lo sviluppo di "**Partnership**" e la diffusione di un'ottica di "**Focus sul cliente**" lungo tutta la filiera, e quelli più di stampo intra-aziendale per lo sviluppo della "**Collaborazione tra dipendenti**" e di una "**Forza lavoro multidisciplinare**" per aumentare la resilienza aziendale, oltre al "**Continuous improvement**" e al "**Knowledge management**" per la gestione della conoscenza in ottica di un processo di miglioramento continuo. L'approccio "Strategic alliance program" si focalizza su strumenti di tipo inter-aziendale finalizzati ad ottenere una piena integrazione della filiera intermodale. Ne fanno parte gli strumenti di "**Partnership**" per l'instaurazione di solide relazioni di lungo periodo, quelli di "**Sviluppo della consapevolezza sulla sicurezza con i miei partner**" e di "**Riduzione delle differenze di cultura tra azienda e partner**" che agiscono rispettivamente tramite contratti e training oppure tramite socializzazione informale e sviluppo della fiducia reciproca sulla compatibilità e l'integrazione tra aziende. Su questi 15 strumenti abbiamo focalizzato l'ambito della nostra ricerca, definendo successivamente le prestazioni di sicurezza (e i relativi KPI) su cui questi strumenti possono impattare. Per le prestazioni di sicurezza non abbiamo preso in considerazione solo il focus tradizionalmente analizzato in letteratura, in particolare da Williams et al. (2008) e da IMCOSEC (2010) (corrispondente alla sicurezza di attacchi della Tabella 3), ma

abbiamo preferito avere una visione più ad ampio spettro che comprendesse due differenti filoni di ricerca (da un lato sicurezza preventiva-resilienza, dall'altro attacchi intenzionali-non intenzionali). In Tabella 3 sono schematizzate le prestazioni di sicurezza che abbiamo definito "da attacchi" e "di fornitura".

Tabella 3: Tipologie di sicurezza

	Sicurezza preventiva	**Resilienza**
Attacchi intenzionali	Sicurezza da attacchi	Sicurezza di fornitura
Attacchi non intenzionali		

In linea con IMCOSEC (2010) il KPI scelto per la sicurezza da attacchi è stato il numero di furti/manipolazioni subiti mentre per la sicurezza di fornitura è stato individuato il ritardo subito, il ritardo causato e il ritardo al cliente finale provocato da tutti gli attori della filiera. Inoltre per considerare la relazione causa-effetto che collega gli strumenti ai KPI abbiamo definito dei fattori causa che concorrono a spiegare una cattiva prestazione di sicurezza. Passando infine ad approfondire i fattori causa, per quanto riguarda la sicurezza da attacchi ne abbiamo individuate 3 di possibili cause che possono determinare un furto/manipolazione: episodi collusivi tra persone interne e/o esterne all'organizzazione, errori di qualsiasi natura nell'implementazione di procedure di sicurezza predefinite (errore operativo) ed errori imputabili a chi definisce le procedure e le politiche gestionali (errore di pianificazione). Per i ritardi i fattori causa sono stati individuati in: assenza di collaborazione e comunicazione tra partner di filiera, inadeguatezza dei partner di filiera per lacune presenti nelle procedure/politiche gestionali, ed errori operativi e/o di pianificazione dell'azienda di riferimento.

Metodologia di ricerca

Definito il modello teorico di riferimento, abbiamo individuato nel caso di studio la metodologia di ricerca da seguire. Il caso di studio, in linea con la natura della nostra ricerca, include dati quantitativi, qualitativi ed elementi teorici e ha l'obiettivo di sviluppare una teoria capace di spiegare i dati raccolti proponendo dei risultati finali di tipo descrittivo (Yin, 2011). Formalmente abbiamo seguito la modalità del caso di studio multiplo (più casi presi in esame) descrittivo (caso sviluppato a valle della definizione del disegno di ricerca) strumentale (funzione di conferma e verifica della

capacità di una teoria pre-esistente di spiegare un determinato fenomeno), in accordo con Yin (2011) e Stake (1995).

In fase preliminare abbiamo delimitato l'unità sulla quale abbiamo concentrato le nostre analisi scegliendo di intervistare un campione d'aziende operante nel settore intermodale il più eterogeneo possibile rispetto ai fattori di contesto individuati. iferendoci allo schema in Figura 1, abbiamo intervistato 10 MTO, di cui 5 con vettori stradali interni e 7 gestori di terminal intermodale di cui 3 con ulteriore ruolo di operatore commerciale del trasporto ferroviario. Considerata la natura dello studio, abbiamo scelto la modalità dell'intervista personale finalizzata alla compilazione di un questionario per verificare che i manager fossero allineati agli obiettivi del nostro studio. L'intervista si è articolata in un'analisi puntuale di ogni strumento da noi proposto per capirne la tipologia di applicazione in azienda e, in caso di applicazione, le aree d'impatto (positivo o negativo) sulle prestazioni di sicurezza da attacchi e di fornitura. Infine abbiamo rilevato la percezione d'importanza che i manager hanno rispetto agli strumenti proposti, e rispetto ai fattori causa che determinano una cattiva prestazione di sicurezza. Dopo le prime interviste effettuate abbiamo riscontrato quali fossero le difficoltà maggiori per i nostri interlocutori nella compilazione del questionario; sulla base di queste abbiamo accorpato gli strumenti "competenza dei dipendenti sulle tematiche di sicurezza" e "consapevolezza interna sulla sicurezza" in un unico strumento "sviluppo della consapevolezza interna sulla sicurezza" (la differenza tra i due non era infatti percepita) e siamo convenuti nell'utilizzare come unico KPI per la sicurezza di fornitura il "ritardo al cliente finale". Il risultato delle 13 interviste effettuate ci ha consentito di mappare la situazione as-is rispetto all'utilizzo e all'impatto che gli strumenti proposti hanno sulla security aziendale e ci ha fornito la base informativa per consentirci di rispondere alle 5 domande di ricerca.

In Tabella 4 sono riassunte le caratteristiche delle aziende del campione intervistato.

Tabella 4: Campione di aziende intervistate classificate in base ai fattori di contesto

Aziende	Fattori di contesto					
	Dimensione	Ambito	Ruolo	Integrazione verticale	Tipologia di merce	Internazio-nalizzazione
AMBROGIO	grande	strada-ferrovia	MV+GO	alta	A	INT
BAS LOGISTICS	piccola	strada	MV	bassa	A+P	INT
EWALS INTERMODAL	grande	strada	M	bassa	A+P	INT
FERCAM	grande	strada	M	bassa	A+P	INT
HOYER GROUP	grande	strada	MV	bassa	P	INT
HUPAC	grande	ferrovia	GO	alta	A+P	INT
INTERPORTO RIVALTA SCRIVIA	grande	strada-ferrovia	M+G	alta	A+P	INT
MARENZANA	piccola	strada	MV	bassa	P	INT
MAGAZZINI DESIO BRIANZA	piccola	strada-ferrovia	M+G	alta	N	INT
SOGEMAR	grande	strada-ferrovia	MV+GO	alta	A+P	INT
TI.MO.	piccola	ferrovia	G	bassa	A+P	ITA
TERMINALI ITALIA	piccola	ferrovia	G	bassa	A+P	ITA
VOTG	grande	strada	M	alta	P	INT
LEGENDA:	M = MTO, MV = MTO e vettore stradale, G = gestore terminal, GO = gestore terminal e operatore commerciale, P = merce pericolosa, A = merce ad alta appetibilità, N = merce non pericolosa e poco appetibile					

Per il fattore dimensione ci siamo riferiti alla definizione della Commissione Europea 6 maggio 2003, n. 2003/361/Ce; per l'integrazione verticale abbiamo considerato integrate quelle aziende che svolgono almeno un ruolo sia nell'ambito stradale che in quello ferroviario, oppure, nel caso presenti solo in ambito ferroviario, se completamente integrate lato rotaia (G + GO + trazionista ferroviario). Dall'analisi delle caratteristiche del campione abbiamo ritenuto non utile, data la bassa eterogeneità, considerare nello studio di caso due fattori di contesto concentrandoci su dimensione, ambito, ruolo e integrazione verticale.

Risultati

In riferimento alla prima domanda di ricerca, ossia quali strumenti culturali da noi proposti vengano effettivamente applicati in azienda, si evince come tre strumenti vengano utilizzati molto meno rispetto a tutti gli altri. In Figura 8 è riportato il grafico che, sulla base del campione completo di aziende intervistate, differenzia tutti gli strumenti da noi proposti in termini di utilizzo e importanza percepita dalle aziende.

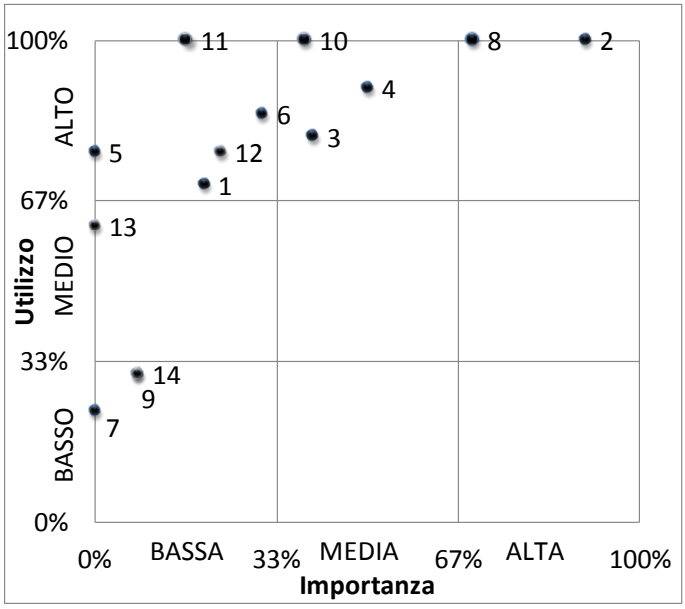


Figura 8: utilizzo/importanza-totale

(1) Forza lavoro multidisciplinare
(2) Collaborazione tra dipendenti
(3) Integrità, lealtà dei dipendenti
(4) Sviluppo della consapevolezza interna sulla sicurezza
(5) Aspetti soft
(6) Continuous improvement
(7) Business continuity planning
(8) Segnalare incidenti e debolezze
(9) Knowledge management
(10) Valutazione della conformità di sicurezza
(11) Partnership
(12) Sviluppo della consapevolezza sulla sicurezza con i miei partner
(13) Riduzione della differenza di cultura tra aziende e partner
(14) Focus sul cliente

Gli strumenti appartenenti al quadrante basso utilizzo-bassa importanza sono: il Business Continuity Planning, per motivi legati alla difficoltà di applicazione nel settore dato il numero troppo elevato di variabili da prevedere e il basso controllo che le aziende possono esercitare sugli altri attori della filiera (in particolare verso il trazionista); il Knowledge Management, di più facile applicazione in settori puramente human intensive e il Focus sul cliente per motivi legati alla natura della filiera intermodale (molto spezzettata) e alla mancanza di un sistema di incentivazione tale da garantire in tutti gli anelli un'attenzione particolare alla buona riuscita dell'intero processo di filiera. In risposta alla seconda domanda di ricerca, cioè capire il possibile impatto che gli strumenti culturali proposti hanno sulle prestazioni di sicurezza, abbiamo creato due mappe causali che evidenziano le relazioni tra strumenti culturali e KPI di sicurezza, passando attraverso gli impatti e i pesi dei fattori causa.

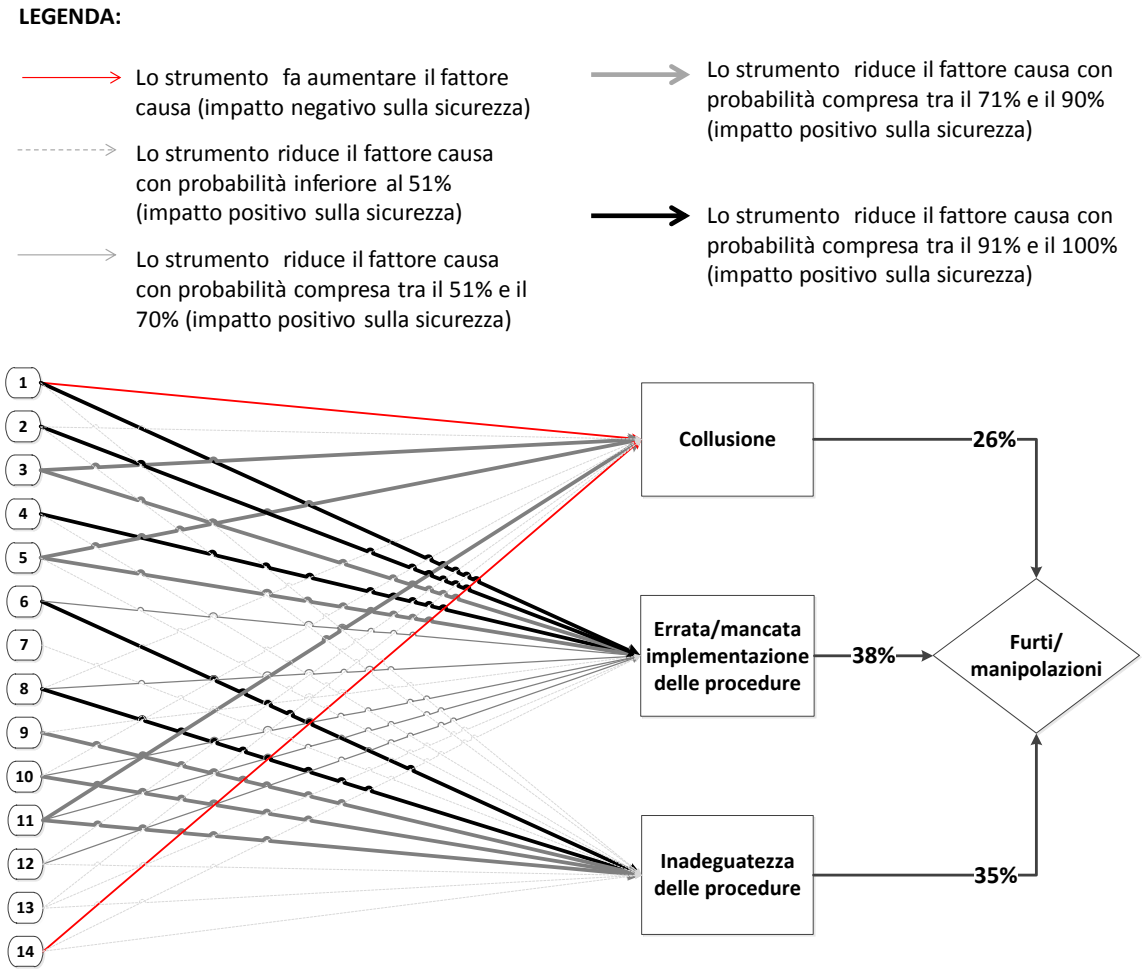


Figura 9: mappa causale-totale-attacchi

Dalla mappa in Figura 9 si evince come le cause dei furti o manipolazioni siano equilibrate. La collusione è quella leggermente meno importante nonostante la forza lavoro multidisciplinare e il focus sul cliente risultino avere impatti negativi su di essa. Questo significa che le aziende riescono a gestire al meglio il trade-off provocato da questi strumenti sulla prestazione di sicurezza. Nonostante molti strumenti abbiano impatti sull'errata e mancata implementazione delle procedure, questa risulta essere la causa principale sulla prestazione di sicurezza da attacchi. In generale, dalle interviste è emerso che le aziende sono ben preparate a limitare episodi di furti e manipolazioni.

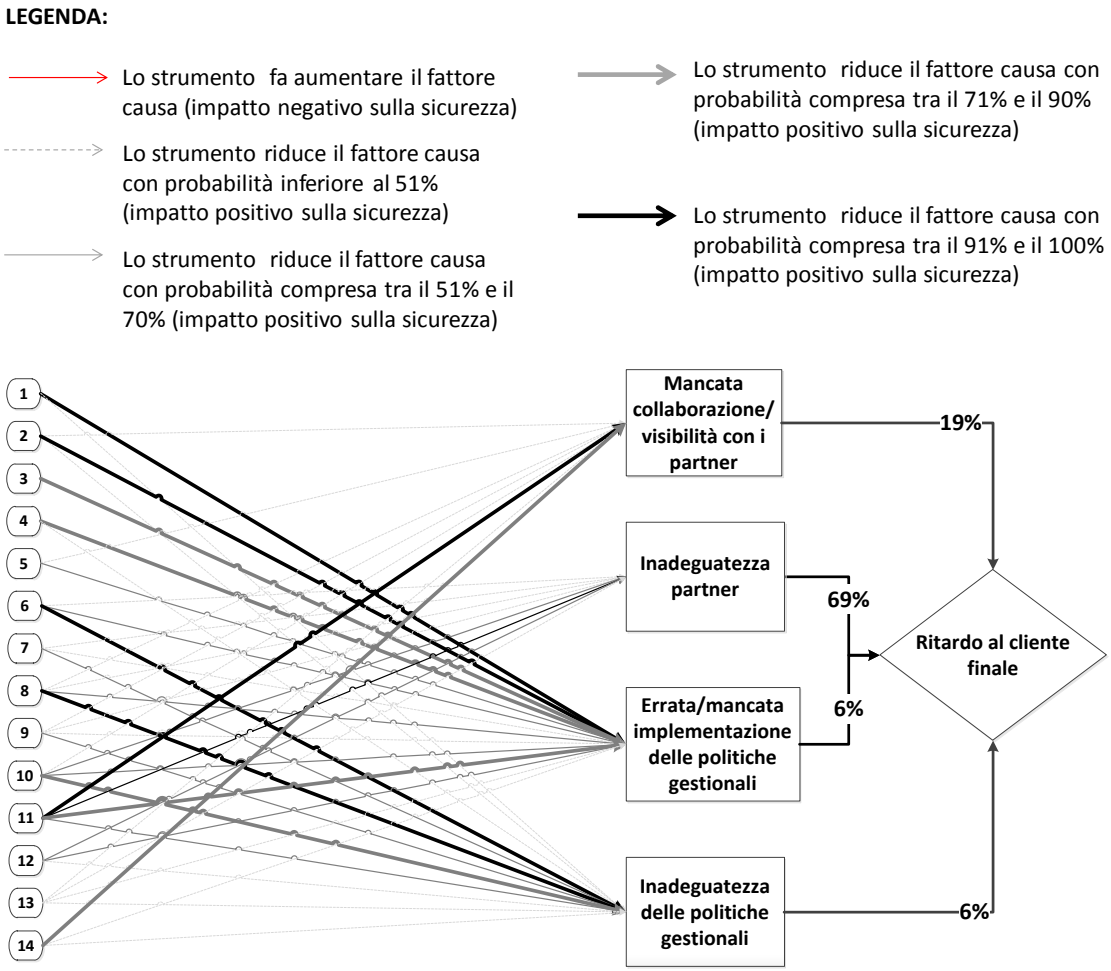


Figura 10: mappa causale-totale-fornitura

Dalla mappa in Figura 10 si evince come il problema principale per le aziende che si occupano di intermodale risieda nel rapporto con i partner di filiera. Analizzando gli impatti degli strumenti si può vedere come questi siano modesti proprio su quei fattori causa "esterni" (mancanza di collaborazione e inadeguatezza del partner) che concorrono maggiormente ad una cattiva prestazione di sicurezza di fornitura. Il motivo risiede nel fatto che è presente una disparità tra l'utilizzo di strumenti interni ed esterni. I primi vengono largamente utilizzati dalle aziende che, per retaggi storici e culturali, sono spinte a focalizzarsi sui processi e le prestazioni interne. Sono presenti invece delle lacune riguardo l'utilizzo di strumenti esterni e questo si traduce in elevati impatti che i fattori causa esterni hanno sulla prestazione finale (per la visione delle diverse mappe causali in funzione dei fattori di contesto si rimanda all'Appendice E).

In relazione alle restanti domande di ricerca abbiamo condotto le medesime analisi suddividendo il campione di aziende in base ai diversi fattori di contesto. I risultati

finali forniscono una panoramica generale sulle differenze di utilizzo degli strumenti culturali proposti in funzione dei diversi fattori di contesto aziendali.

Si denota, come si poteva presumere, che le aziende di dimensioni più elevate sono spinte verso un utilizzo ed una formalizzazione (intesa come standardizzazione della modalità di utilizzo) degli strumenti maggiore (in media vengono applicati dalle grandi aziende 11,75 strumenti su 14 proposti di cui 9,3 in modo formale, mentre per le piccole questo dato scende a 8,2 di cui 4,4 in modo formale). Questo fenomeno è dovuto alla maggiore complessità interna di queste aziende, per le quali risulta difficile poter raggiungere obiettivi di sicurezza senza l'utilizzo formale degli strumenti proposti. Un ulteriore motivo di questa discrepanza tra piccole e grandi aziende risiede nel fatto che la maggior dimensione, con conseguente maggior strutturazione, maggior volume d'affari e maggior potere contrattuale, pone le grandi aziende in una posizione privilegiata nell'applicare gli strumenti proposti.

Per quanto riguarda l'integrazione invece, non c'è una così netta differenza nell'utilizzo degli strumenti proposti (le aziende con alta integrazione applicano in media circa 11 strumenti dei 14 proposti, di cui 8,4 formalmente, contro i 9,57 delle aziende con bassa integrazione, di cui circa 6 formalmente). L'integrazione risulta un fattore discriminante soltanto per due strumenti: la forza lavoro multidisciplinare (anche se spiegata meglio dall'ambito) e il BCP.

Passando al fattore di contesto ambito abbiamo notato come tutti quegli strumenti esterni legati alle prestazioni di filiera vengano maggiormente implementati dalle aziende stradali, il riferimento è in particolare agli strumenti 12-sviluppo della consapevolezza sulla sicurezza con i miei partner, 13-riduzione della differenza di cultura tra azienda e partner e 14-focus sul cliente i quali vengono in media applicati dal 72% delle aziende con interfaccia stradale contro il 33% di quelle ad interfaccia ferroviaria. La motivazione che spinge le aziende ad applicare questi strumenti è la responsabilità sulle prestazione che detengono di fronte al cliente finale; essendo la loro interfaccia, chi lavora in ambito stradale ha sviluppato maggiormente il senso di appartenenza ad un'unica filiera e si impegna nel ridurre le differenze culturali, sviluppare le competenze e la consapevolezza sulle tematiche di sicurezza così da raggiungere elevati target prestazionali (acquisendo così credibilità e fiducia dai clienti industriali). Si nota inoltre un'altra differenza tra le aziende appartenenti ad ambiti diversi. Da un lato le aziende con interfaccia ferroviaria hanno la necessità di impiegare una forza lavoro multidisciplinare (il 67% contro il 33% in ambito stradale), dato

l'elevato numero di mansioni operative svolte all'interno del terminal intermodale (basti pensare ai diversi controlli da effettuare contestualmente all'arrivo e al trasbordo delle ILU); dall'altro le aziende che lavorano in ambito stradale applicano in modo più strutturato e formale gli strumenti legati allo sviluppo delle competenze di sicurezza (100% formale contro il 33% in ambito ferroviario) e alla segnalazione di incidenti (83% formale contro 33% in ambito ferroviario). Questa tendenza è dovuta al fatto che in ambito stradale esiste una maggior variabilità del rischio di incorrere in una disruption rispetto all'ambito ferroviario (in un terminal tutte le attività sono svolte in un unico sito, mentre una società di trasporti su gomma per sua stessa natura svolge le sue attività in siti differenti ed è quindi esposta a maggiori rischi).

Oltre a svolgere le analisi prendendo in considerazione un fattore di contesto per volta, abbiamo ritenuto interessante svolgere un'analisi incrociata combinando tra loro tutti i possibili fattori di contesto ottenendo così otto diversi cluster. Qualsiasi azienda operante nel settore intermodale può quindi essere ricondotta ad uno specifico cluster in funzione dei suoi specifici fattori di contesto. Il risultato di questa analisi incrociata ha portato all'elaborazione di otto diverse check-list di strumenti culturali (in Figura 11 e Figura 12) che consentono ad una generica azienda di raggiungere prestazioni di sicurezza (da attacchi e di fornitura) in linea con il settore. Questo non vuol dire avere delle performance di sicurezza ottimali perché, se da un lato le prestazioni del settore sono buone per la sicurezza da attacchi (per le aziende intervistate i furti/manomissioni risultano essere in numero limitato), ciò non è vero per quella di fornitura. Come si evince dalla Figura 10, vi è una netta differenza tra i fattori causa intra-aziendali e quelli inter-aziendali; questo ci suggerisce che il settore presenta una buona sicurezza interna e delle lacune su quella esterna, lasciando elevati margini di miglioramento per quello che riguarda il rapporto con i partner di filiera. Riteniamo che utilizzando in modo più strutturato gli strumenti esterni da noi proposti - che dalle analisi iniziali sul totale del campione risultano i meno utilizzati e ritenuti meno importanti - si possa diminuire in modo significativo il ritardo al cliente finale raggiungendo così una prestazione di sicurezza di fornitura elevata.

Dimensione grande												
Strada						Ferrovia						
alta integrazione verticale			bassa integrazione verticale			alta integrazione verticale			bassa integrazione verticale			
Check-list strumenti per cluster A			**Check-list strumenti per cluster C**			**Check-list strumenti per cluster E**			**Check-list strumenti per cluster G**			
Comuni	2	Collaborazione tra dipendenti	Comuni	2	Collaborazione tra dipendenti	Comuni	2	Collaborazione tra dipendenti	Comuni	2	Collaborazione tra dipendenti	
	3	Integrità, lealtà dei dipendenti		3	Integrità, lealtà dei dipendenti		3	Integrità, lealtà dei dipendenti		3	Integrità, lealtà dei dipendenti	
	5	Aspetti soft		5	Aspetti soft		5	Aspetti soft		5	Aspetti soft	
	6	Continuous improvement		6	Continuous improvement		6	Continuous improvement		6	Continuous improvement	
	8	Segnalare incidenti e debolezze		8	Segnalare incidenti e debolezze		8 (n.f)	Segnalare incidenti e debolezze		8 (n.f.)	Segnalare incidenti e debolezze	
	10	Valutazione della conformità di sicurezza		10	Valutazione della conformità di sicurezza		10	Valutazione della conformità di sicurezza		10	Valutazione della conformità di sicurezza	
	11	Partnership		11	Partnership		11	Partnership		11	Partnership	
Caratteristici	**4**	**Sviluppo della consapevolezza interna sulla sicurezza**	**Caratteristici**	**4**	**Sviluppo della consapevolezza interna sulla sicurezza**	**Caratteristici**	**1**	**Forza multidisciplinare**	**Caratteristici**	**1**	**Forza multidisciplinare**	
	7	**Business continuity planning**		**9 (n.f.)**	**Knowledge management**		**4 (n.f.)**	**Sviluppo della consapevolezza interna sulla sicurezza**		**4 (n.f.)**	**Sviluppo della consapevolezza interna sulla sicurezza**	
	9 (n.f.)	**Knowledge management**		**12**	**Sviluppo della consapevolezza sulla sicurezza con i miei partner**		**7**	**Business continuity planning**		**9 (n.f.)**	**Knowledge management**	
	12	**Sviluppo della consapevolezza sulla sicurezza con i miei partner**		**13**	**Riduzione della differenza di cultura tra aziende e partner**		**9 (n.f.)**	**Knowledge management**	Non utilizzati	7	Business continuity planning	
	13	**Riduzione della differenza di cultura tra aziende e partner**		**14 (n.f.)**	**Focus sul cliente**	Non utilizzati	12	Sviluppo della consapevolezza sulla sicurezza con i miei partner		12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	
	14 (n.f.)	**Focus sul cliente**	Non utilizzati	1	Forza multidisciplinare		13	Riduzione della differenza di cultura tra aziende e partner		13	Riduzione della differenza di cultura tra aziende e partner	
Non utilizzati	1	Forza lavoro multidisciplinare		7	Business continuity planning		14	Focus sul cliente		14	Focus sul cliente	

Figura 11: check-list strumenti culturali per aziende grandi

Dimensione piccola												
Strada						Ferrovia						
alta integrazione verticale			bassa integrazione verticale			alta integrazione verticale			bassa integrazione verticale			
Check-list strumenti per cluster B			**Check-list strumenti per cluster D**			**Check-list strumenti per cluster F**			**Check-list strumenti per cluster H**			
Comuni	2 (n.f.)	Collaborazione tra dipendenti	Comuni	2 (n.f.)	Collaborazione tra dipendenti	Comuni	2 (n.f.)	Collaborazione tra dipendenti	Comuni	2 (n.f.)	Collaborazione tra dipendenti	
	3 (n.f.)	Integrità, lealtà dei dipendenti		3 (n.f.)	Integrità, lealtà dei dipendenti		3 (n.f.)	Integrità, lealtà dei dipendenti		3 (n.f.)	Integrità, lealtà dei dipendenti	
	5 (n.f.)	Aspetti soft		5 (n.f.)	Aspetti soft		5 (n.f.)	Aspetti soft		5 (n.f.)	Aspetti soft	
	6 (n.f.)	Continuous improvement		6 (n.f.)	Continuous improvement		6 (n.f.)	Continuous improvement		6 (n.f.)	Continuous improvement	
	8	Segnalare incidenti e debolezze		8	Segnalare incidenti e debolezze		8 (n.f.)	Segnalare incidenti e debolezze		8 (n.f.)	Segnalare incidenti e debolezze	
	10 (n.f.)	Valutazione della conformità di sicurezza		10 (n.f.)	Valutazione della conformità di sicurezza		10 (n.f.)	Valutazione della conformità di sicurezza		10 (n.f.)	Valutazione della conformità di sicurezza	
	11	Partnership		11	Partnership		11	Partnership		11	Partnership	
Caratteristici	**4 (n.f.)**	**Sviluppo della consapevolezza interna sulla sicurezza**	**Caratteristici**	**4 (n.f.)**	**Sviluppo della consapevolezza interna sulla sicurezza**	**Caratteristici**	**1 (n.f)**	**Forza multidisciplinare**	**Caratteristici**	**1 (n.f.)**	**Forza multidisciplinare**	
	12 (n.f.)	**Sviluppo della consapevolezza sulla sicurezza con i miei partner**		**12 (n.f.)**	**Sviluppo della consapevolezza sulla sicurezza con i miei partner**	Non utilizzati	4	Sviluppo della consapevolezza interna sulla sicurezza	Non utilizzati	4	Sviluppo della consapevolezza interna sulla sicurezza	
	13 (n.f.)	**Riduzione della differenza di cultura tra aziende e partner**		**13 (n.f.)**	**Riduzione della differenza di cultura tra aziende e partner**		7	Business continuity planning		7	Business continuity planning	
Non utilizzati	1	Forza multidisciplinare	Non utilizzati	1	Forza multidisciplinare		9	Knowledge management		9	Knowledge management	
	7	Business continuity planning		7	Business continuity planning		12	Sviluppo della consapevolezza sulla sicurezza con i miei partner		12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	
	9	Knowledge management		9	Knowledge management		13	Riduzione della differenza di cultura tra aziende e partner		13	Riduzione della differenza di cultura tra aziende e partner	
	14	Focus sul cliente		14	Focus sul cliente		14	Focus sul cliente		14	Focus sul cliente	

Figura 12: check-list strumenti culturali per aziende piccole

Come complemento alle check-list, abbiamo inoltre riassunto le best practice che durante le interviste sono emerse riguardo l'applicazione degli strumenti culturali proposti. In ultima istanza abbiamo riassunto i temi trasversalmente riscontrati nel corso delle interviste rispetto alla gestione del servizio intermodale e al suo sviluppo futuro. Questi temi sono:

- il ruolo delle informazioni. Si evince come, oltre ai benefici descritti in letteratura, ci siano anche dei potenziali rischi associati all'aumento di episodi collusivi;
- il vantaggio dell'integrazione verticale. È la tendenza delle più grandi imprese del settore che ne riconoscono i vantaggi in termini di controllo e visibilità sul trasporto end-to-end;
- la focalizzazione del servizio intermodale. Da un lato abbiamo riscontrato una tendenza a differenziare l'offerta di servizi intermodali rispetto alle altre modalità di trasporto per spostare l'attenzione sulle qualità distintive piuttosto che sul mero confronto economico; dall'altro lato la tendenza è quella di specializzarsi su determinate tratte così da ottenere un miglior presidio e un conseguente miglioramento della sicurezza del trasporto;
- la spinta verso la qualità del servizio. Il trasporto intermodale ha degli innegabili vantaggi sulla sicurezza, sull'efficacia e sull'eco-compatibilità. La mancanza di politiche che incentivino queste performance sono allo stato attuale un grosso ostacolo allo sviluppo dell'intermodale.
- la percezione della ferrovia da parte delle industrie e dell'opinione pubblica. Il riferimento è alla situazione italiana che considera la ferrovia come una modalità di trasporto inefficiente e insicura. In realtà il problema è in parte culturale e legato alla tradizione, accentuato da un mancanza di coerenza e di un reale impegno politico per lo sviluppo della ferrovia.

Conclusioni e sviluppi futuri

Il contributo innovativo del nostro lavoro risiede nell'approfondimento, all'interno del filone di studio della Supply Chain Security, di un'area ancora poco sviluppata riferita alla Supply Chain Security Culture. Abbiamo proposto una classificazione strutturata degli strumenti che concorrono allo sviluppo di questo nuovo approccio alla security che non era presente in letteratura.

La metodologia di analisi scelta è differente da quella utilizzata in riferimento ai classici strumenti di security perché, data la natura degli strumenti culturali, non è possibile proporre un approccio basato semplicemente sul rapporto costi-benefici. Il nostro modello teorico di riferimento, che vuole combinare delle informazioni qualitative e quantitative, può essere generalizzato a qualsiasi azienda del settore intermodale. Attraverso una mappatura della situazione as-is è stato possibile individuare delle specifiche chek-list di strumenti culturali per ogni tipologia di azienda; questo benchmark è utile per allineare le prestazioni aziendali di sicurezza con quelle medie del settore. Abbiamo inoltre individuato le aree di miglioramento di queste prestazioni e le attuali best practice del settore. Il limite del modello proposto è da ricercare nel ristretto campione d'aziende che non permette di effettuare delle analisi statistiche robuste; abbiamo effettuato inoltre delle approssimazioni sui parametri del modello data l'impossibilità di accedere ai dati storici presenti nei database aziendali.

Si evidenzia inoltre come si possa condurre un ulteriore studio complementare che consideri le prestazioni organizzative correlate a quella di sicurezza (come schematizzato in Figura 4). Ad ogni modo lo studio ha permesso di rispondere in modo dettagliato a tutte le domande di ricerca proposte.

Executive summary

The field of research[3]

Our thesis deals with the security within the ILU (Intermodal Load Unit) Supply Chain. The term "ILU supply chain" is referred to both companies and players that interact to bring the flow of ILUs (which consists in containers, semi-trailers and swap bodies) from the origin to the final destination (definition taken out of IMCOSEC, 2010).

Within ILU supply chain we focused on the intermodal transport road-rail way, particularly the combined one, where the largest transport is done on rail and the first and last miles is done on road. The typical benefits of this new transport approach are mainly regard the social, security, energy saving, environmental and sustainability aspects. These benefits that go beyond a strict economic analysis has been recognized by European Union which implemented several programs in favor of the intermodal transport. The goal of these programs was to balance the use of the different transport ways (road, rail, maritime, inland waterway, air); today the European transport system is strongly unbalanced toward the road and in general toward the use of assets that are not sustainable both from the environmental and the energetic point of view. At the present time, in the Italian situation the major issues for the development of an intermodal transport system are:

- Lack of infrastructures;
- Lack of management, mainly linked to the specific characteristic of intermodal transport which required the coordination of several players that run different activities. Moreover the intermodal transport is less flexible of the road one, especieally in fouding the load for the way back;
- Lack of legal requirements, particularly about the different status of implementation of the European directives about the deregulations of the rail market in the single countries;
- Lack of a clear rule splitting, particularly about the dominant position of some big companies.

[3] in collaboration with Ing. Fulvio Quattroccolo, founder and manager of the website www.intermodale24-rail.net

The intermodal road-rail transport can be classified according to several features such as the type of ILU transported (containers, semi-trailers and swap bodies), the transport system (accompanied or not accompanied) and the kind of the train used (completed train or single charge train).

The single rules played into the intermodal supply chain, that we have derived by the information gathered during the interviews, are showed in Figure 1.

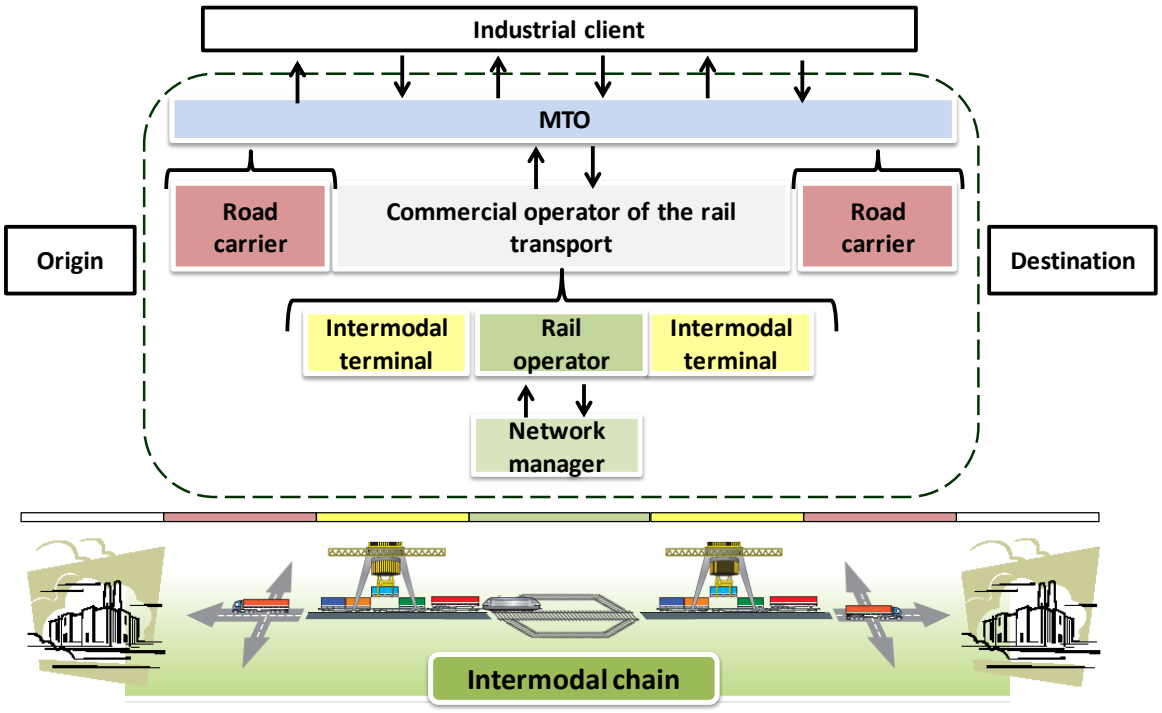


Figure 1: ILU supply chain

Literary Research

Through our literary research, we found out that it doesn't exist an unic meaning of the italian concept of "sicurezza", because it has two different meanings which can be linked to the english words of "security" and "safety". The first it's about the security of tangible or intangible goods, the second one is about security of physical persons. Moreover, the term "sicurezza" can be also interpreted in different ways according to the approach on which can be analyzed that could be: legally, managing, practice, sociologic, organizational, technical, engineering etc. We mainly dealt with the intermodal transport security according to the managing, organizational, sociological and only partly technical.

Even the companies have approached the security concept from different point of view. The first studies were particullarly based on sociological and psicological approach,

focusing on safety and wellness of people. The concern in securing the goods during the transport raised in literature during the last years, with the introduction of the concept of Supply Chain Security (SCS). The term of SCS is referred to an approach that implying the application of programs, systems, procedures and technological solutions able to takle the supply chain threats with the final aim to improve security (Donner and Kruk (2009), Closs and McGarrell (2004), Burmeisters and Solovjovs (2009)).

Since September 11th the awareness of security topics has raised and consequently the approach to SCS has changed. On Figure 2 are summarised the main changes, partly still ongoing.

	Before		After
Measures	Theft prevention	→	Theft prevention and anti-terrorism
Approch	Functional	→	Integrated
Initiatives	Public or private	→	Public and private
Extension	National/local	→	Global
Focus	Company	→	End-to-end supply chain
Visibility	1st-tier suppliers	→	2nd, 3rd-tier suppliers
Support	Contingency Planning	→	Contingency planning & Crisis Mgmt
Impact	Operative	→	Strategic

Figure 2: Evolution of SCS

SCS practices used to be placed within the Risk management system by the companies. This shows how it's important to make an accurate analysis of the risk linked to the supply chain in order to understand what security strategies has to be applied in reducing vulnerability. According to the vulnerability matrix, in which every source of risks is classified by the "likelihood of occurrence" and the the "severity of consequences", the reduction of vulnerability can be achieved by the reduction of both the components. The performance of security is linked to both these variables and, in more in details, it could be described in term of preventive security, as the *"company capability to monitoring and preventing perils compromising its operations"* and resilience, as the *"company capability to bring back the ordinary operations after a disruption"* (Nassimbeni, 2009).

On Figure 3 we observed that the SCS strategies change according to the different supply chain risks and the environmental conditions.

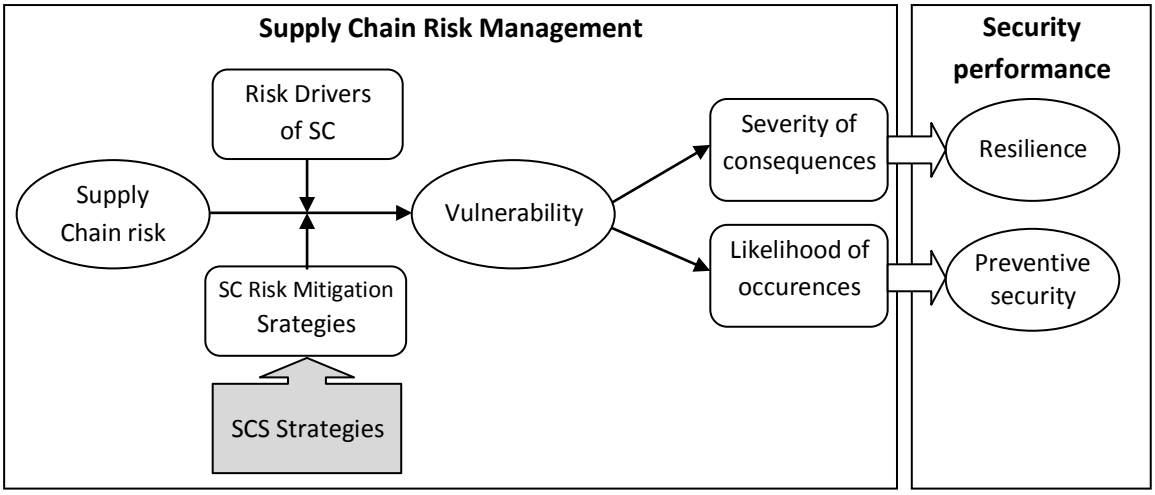


Figure 3: Supply chain risk management and security performance

Recent trends demonstrate how companies have put high attention to risks coming from intentional threats, hence to the strategies which can decrease the probability to make them happen. The SCS strategies may impact also on other organizational performance: they could affect directly security and efficiency, and indirectly on effectiveness; at the same time they could cause trade-off between security and efficiency performance, as showed in Figure 4. Referring to the trade-off, Willis and Ortiz (2004) observed that working under normal operating conditions, a security program could bring negative effect in term of efficiency; Sheffi (2001) and Nassimbeni (2009) identified either some SCS strategies which could bring to a worst level of efficiency, and, on the contrary, supply chain strategies improving efficiency but making worse security.

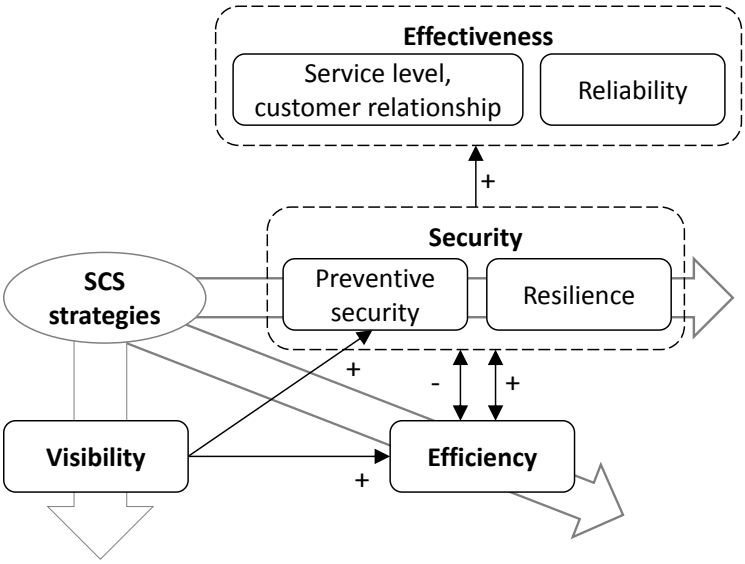


Figure 4: Map of organizational performance

Through the analysis of the relation between SCS and performances, it's showed that the obstacle in spreading of a SCS approach is the lack of quantitative studies which prove the positive impact both on efficiency and effectiveness performing, the trade-off in security and efficiency performance and also the lack of a correct communication of security practices and the difficulty in understanding the obtainable benefits within the supply chain.

Afterwards the SCS approach has been used in our main field, the intermodal transport in the supply chain, defined by some authors as "container supply chain" or more generally as "ILU supply chain".

The companies' globalization is the main reason why public authorities and private organizations has focused on ILU supply chain security. The importance to secure the flow of containers comes from the high risks linked to the intermodal transport: several times containers have been used for the transport of illegal weapons or terrorists, in addition to have been frequently affected by tampering or theft (Sarathy, 2005). ILUs are particularly weak and exposed at the risks in all the step of the chain: production plants, loading units, suppliers, partner and freight operators, logistic facilities, people and information (Sarathy, 2005, 2006).

An additional issue is linked to the implementation of an integrated SCS approach throughout all the supply chain that, together with the lack of risk management culture, don't allow to have a clear knowledge of the risks that supply chain is facing, hence decrease the necessary condition for reduce vulnerability (Williams et al., 2008; IMCOSEC, 2010).

With the increasing importance of SCS topics, authorities and private companies have suggested programs to secure the supply chain. In comparison to the traditional focus, these new programs consider the whole supply chain, proposing a cooperation program between private companies and authorities. (Donner and Kruk, 2009).

Table 1 summarized the most important voluntary programs sponsored over the last years.

Table 1: Major voluntary programs

Name/year started	Originated Country/ Institute	Mode	Participation/ status	Category	Goal
TAPA, 1997	US	Road	207 members	Private voluntary	Crime incident reporting/identify solutions/share information
C-TPAT, 2001	US	All	6375 certified and 3916 validated companies	Government voluntary	Supply chain security
CSI, 2002	US	Sea	58 ports	Government voluntary	Supply chain security
WCO SAFE FoS, 2005	WCO	All	156 member States	International voluntary	Standard for SCS and trade facilitation
ISO 28000, 2005	ISO Technical Committee	All	157 member States	International voluntary	Supply chain security
EU-AEO, 2008	European Commission	All	192 companies	Government voluntary	Supply chain security and trade facilitation

New approaches are focused on security with the goal to spread the international standards, to diffuse and share information between private companies and authorities, to develop a performing security management systems and develop a process which allow an integrated management of the chain (Gutierrez and Hintsa, 2006).

Through the analysis of the most important international programs and literature about SCS practices, we have developed the follow classification on security tools, represented in Figure 5.

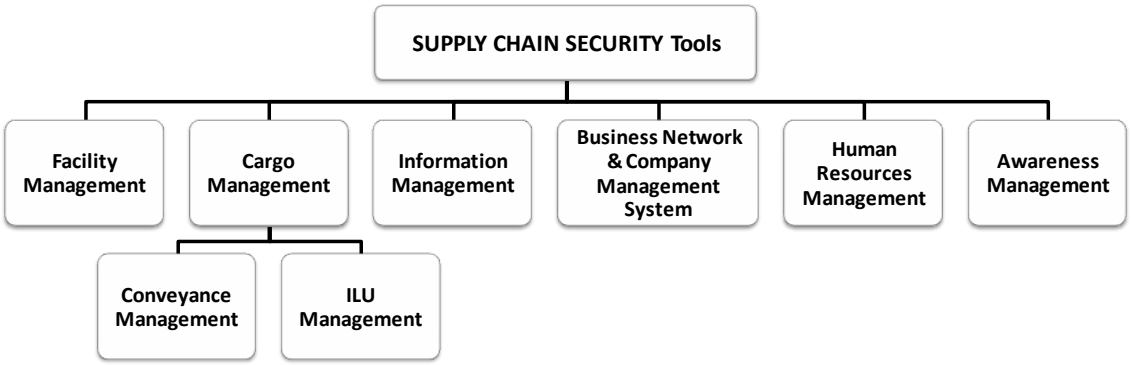


Figure 5: Classification of SCS tools

Within the "Facility Management" category there tools for securing those assets used for storage and management of ILUs. Some of these tools acts in the designing stage in order to reduce the risks affecting the facility, others to provide the physical security and, at last, others to monitor the access and identifications of people and vehicles. "Cargo Management" tools guarantee the security of the cargo during all the steps of the transport. In this category we can distinguish tools directly linked to the transport

devices ("Conveyance Management") from the others which guarantee the security of ILUs from intentional threats ("ILU Management"). The first category includes planning of inspection during the transport, tracking solutions and the route management of cargo. The second category includes techniques and technologies to check ILUs and anti-tampering solutions, both considered by the technological and process/organizational aspect. "Information Management" tools allow a correct use of the available information as a way to find out issues, to prevent security breaches and to protect the critical information of the business. All these tools allow companies to build up a very high quality database and to adopt practices for the information security and the know-how management. "Business Network & Company Management System" tools allow to secure the company management system, particularly in the design and implementation of a corporate security system and, in particular, of a flexible and resilient logistic system. In addition, these tools enable the supply chain partners' evaluation and the setting up of a cooperative relationship with companies and authorities.

"Human Resource Management" tools guarantee the reliability of people who are in contact with ILUs, by acting on the hiring and exit process of people and on the security rules and responsibilities fixed in the company. Finally, "Awareness Management" tools guarantee the awareness about security of all the people that are in contact with ILUs. They include initiatives settled to training and educate employees and to the development of the knowledge about security topics both within the companies and the partners among the chain.

Research design

Through a literary research about SCS, we found out a group of tools less studied than others, belonging to the "Information", "Human Resource" and "Awareness Management" categories. Those categories has the common characteristic to be not strictly linked to a specific process or step within the supply chain, but to be best linked to human factors, so that we decided to define these tools as "cultural" because they act on values, motivations, attitudes and behaviors of people within the company. Considering the low level of examination of these tools by authors, their cross-funtionality and the importance of the human factor related to security (Lacey, 2010), we decided to focus our study on them.

In order to narrow our research, we have focused on the concept of organizational culture and its implementation among companies referring it to the security point of view. We learned that the concept of Supply Chain Security Culture (SCSC) and Supply Chain Security Orientation (SCSO) has been spread over companies recently (Benson, 2005; Autry e Bobbitt, 2008; Williams et al., 2008). The spreading of this practices comes from the combination of several factors such as the increasing focus of the SCS topics from authorities and private companies, the importance of the role of cultural topics in affecting strategic, tactic and operatives objectives and the better awareness that people and companies are both the major players in generating disruption and, at the same time, the most important means to avoid them and restrain consequences (Lacey, 2010). Taking into account these considerations, we decided to studying the role of the cultural tools in improving the ILU supply chain security. At this stage, we narrowed our study through the definition of 5 research questions:

1. What cultural tools are implemented by companies that work in the intermodal sector?
2. What is the impact of the application of every tool on security performance?
3. There are contingency factors which can explain the adoption of cultural tools?
4. The contingency factors can explain also the impact of these tools on performance?
5. What are the most important reasons which determine a bad security performance? Are they different according to the contingency factors?

While for the answer of the first research question could be enough to collect the information from the interviewers, instead, for the other questions it was necessary to build a theoretical model, represented in Figure 6, based on four correlated components.

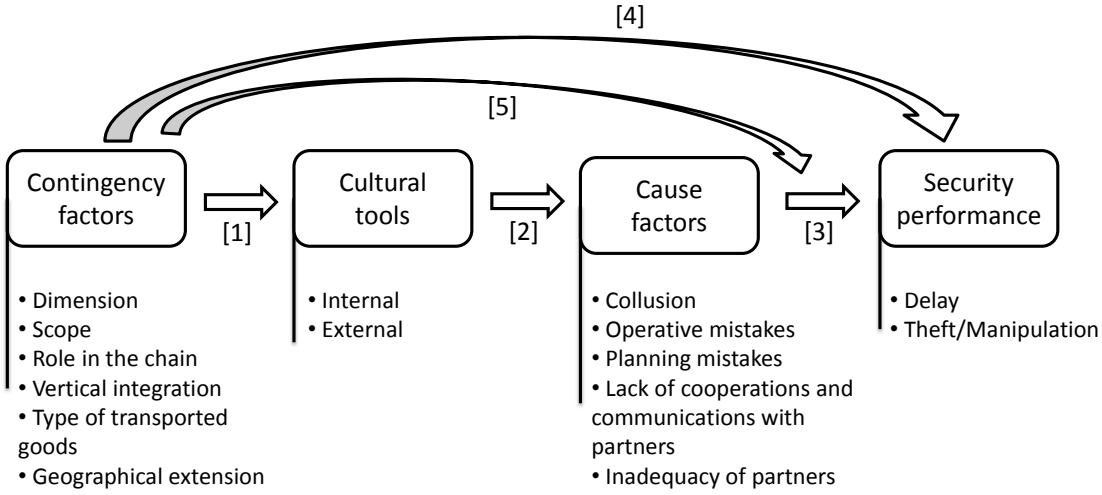


Figure 6: theoretical model

Referring to Figure 6, the relations [1] assumes the presence of some discriminant contingency factors in the use of a specific cultural tools (answering the research question n°3); relation [2] shows the potential impact of a single cultural tool on a specific cause factors that affect the final security performance [3] (relation [3] describes the relative importance of the cause factors, related to the security performance and it allows to answer at the first part of the research question n°5). The remaining relations assume that the impact of the cause factors [5] and of the tools [4] on security performance may vary according to the contingency factors (the relations allows to answer respectively to research question n°4 and n°5). In order to answer the research question n°2, it will be necessary to match relations [2] and [3], and so to understand the impact that every tool has on security.

The contingency factors included in the model, allow to define the company profile and consist in: dimension (big, small), scope (road, rail, both), role of intermodal chain (MTO, road carrier, terminal manager, commercial operator of the rail transport), vertical integration (high, low) type of transported goods (dangerous, desirable, others) and geographical extension (international, national).

Moving on the cultural tools, we took account of the analysis of the literature about SCSC, in which no one proposed a classification of this tools' category and for this reason we suggested a new classification based on four security culture approaches, described in Figure 7.

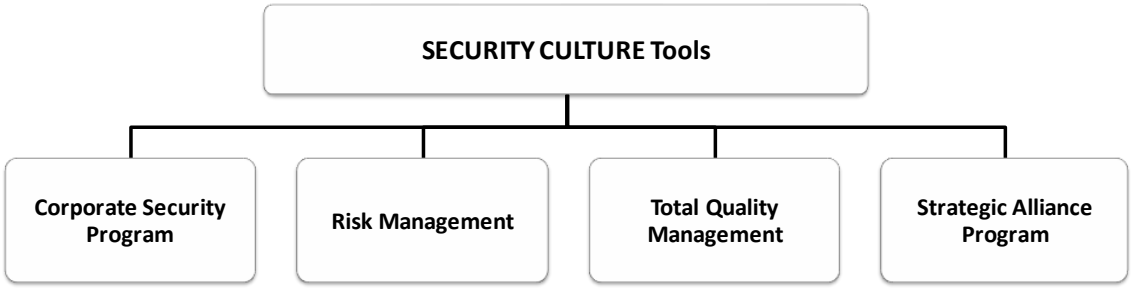


Figure 7: Classification of SCSC tools

In Table 2 it is fully described the SCSC tools identified.

Table 2: SCSC tools

CORPORATE SECURITY PROGRAM	Integrity, loyalty of employees	Past's investigation and interview with potential employee and third part employee
		Loyalty employee's program
		HR policy
		Span of control
	Employee know how about security topics	Involvement of outside expertise
		Employee training
		Teamwork
	Awareness about security	Assigning security responsibilities to personnel
		Incentive system and feedback on security performances
		Punishments
		Organizational changes program
		Informal socialization
		Internal communication
		Security function/position (CSO)
	Soft aspects	Symbolism
		Motto
		Code of conduct
RISK MANAGEMENT	Business continuity planning	Employee training
		Employee empowerment
		Action plan
	Report incidents and weaknesses	Analysis of the nature and causes of incidents
		"Swiss Cheese" model
		"Near misses" monitoring
	Assessing of security compliance	Preventive tools based on real security experience
		Certifications
TOTAL QUALITY MANAGEMENT	Partnership	Cooperation norms
		Long term relationship
		Share risks, awards and responsibilities
		Trust development
	Employees cooperation	Share risks, awards and responsibilities
		Teamwork
	Multitask working force	Cross-functional interaction
		Hire personnel with specific security skills
		Employee training
	Continuous improvement	Security function/position (CSO)
		Top management support
		Monitoring of existing process
		Employee empowerment
	Customer focus	-
	Knowledge management	Inter-firm learning
		Institutionalization of knowledge
STRATEGIC ALLIANCE PROGRAM	Awareness development of security with partners	Inter-firm learning
		Contract with specific security requirements
		Partner education
	Reduction of cultural differences between company and partners	Trust development
		External communication
		Hibridal cultural interface (HCI)
		Informal socialization
	Partnership	Cooperation norms
		Long term relationship
		Share risks, awards and responsibilities
		Trust development

The "Corporate Security Program" approach led to the design of a structure plan for the development and spreading of the security culture over the company. These tools are intra-company and they split into programs of "**Integrity and loyalty of employees**" that can be used for the selection and loyalty of people, "**Employee know how about security topics**" and "**Awareness about security**" that act on the education, training and diffusion of the security topics, and finally the "**Soft aspects**" that mean to create an organizational culture able to influence the daily practice work by acting on philosophy, ideology, values and people expectations. The second approach consist in the "Risk Management", which includes cultural tools that support the management of companies vulnerabilities. This approach is based on "**Business Continuity Planning**" tools that describe the way a company can turn back its critical operations as operative after a disruption, the "**Reporting of accident and weakness**" tools for the analysis of the nature of accident/near misses happened and the "**Assessing of security compliance**" tools for the checking of conformity toward security requirements. The third approach, is focused on the tools that are traditional classified as "soft TQM". In this approach there are inter-company tools for the implementation and the development of "**Partnership**" and the diffusion of a "**Costumer focus**" point of view along the supply chain, and also some intra-company tools for the development of the "**Employees cooperation**" and of a "**Multitask working force**" to improve the company resilience, additionally to the "**Continuous improvement**" and "**Knowledge management**" for the know-how management by a continuous development process view. Finally, the "Strategic alliance program" approach is focused on inter-company tools which aim is to achieve a complete integration over the intermodal chain. This approach includes "**Partnership**", "**Awareness development of security with partners**" and "**Reduction of cultural differences between company and partners**", respectively acting on contracts and training, or by informal socialization and development of trust and integrations between companies.

We focused our research on these 15 tools an we consequently defined the security performances (and relative KPIs) on which these tools may impact. About security performances we did not take account of only the traditional focus considered by literature (in particular by Williams et al., 2008 and IMCOSEC, 2010) that correspond in "attacks" security showed in figure 2; on the contrary we preferred to have a broad vision which could include the two different research point of view consisted on one hand in preventive security/resilience and on another hand in intentional/not intentional

attacks. Table 3 summarized the security performances that we have defined "attacks" security and "supply" security.

Table 3: Type of security performance

	Preventive security	**Resilience**
Intentional Attacks	"Attack"security	"Supply" security
Unintentional Attacks		

We chose the number of thefts/manipulations to represent the KPI of "attack" security (according to IMCOSEC, 2010), and the passive delay from supplier, the active delay to client, and the sum of both caused to the final costumer from all the player in the chain to represent the "supply" security ones. Moreover, in order to consider the cause-effect relation between tools and KPIs, we defined some cause factors that contribute to explain a bad security performance.

Moving on the close examination of the cause factors, referring to the security "attack" security we have found out 3 potential reasons why a thefts or manipulation could happen; these are the collusion between internal and external people, the operative mistakes and the planning mistakes. With regards to the delays affecting Acthe "supply" security, the reasons could be the lack of cooperation and communication between supply chain partners, the inadequacy of the chain partners, the operative mistakes and the planning mistakes made by the management.

Research methodology

After defining the theoretical model, we referred our research methodology to the case study approach. The case study, in line with the scope of our research, includes quantitative data, qualitative and theoretical elements and is aimed at developing a theory able to explain the collected data and to suggest a descriptive final outcome (Yin, 2011). According to Stake (1995) and Yin (2011), we formally followed the multiple (taking in exam more cases of study), descriptive (the case has been developed after defining the research design) and instrumental (with the purpose to approve and assess the capacity of a pre-existing theory to explain a phenomenon) type of case of study. Preliminary, we focused to run our interviews on a heterogeneous target of companies

operating in the intermodal sector, in relation to the contingency factors we have identified.

As regards with Figure 1, we interviewed 10 MTO, 5 of which with internal road carrier and 7 intermodal terminal administrators, 3 of which with the additional role of commercial operator of rail transport.

Considering the nature of our study, we chose to have a personal interview finalized to fill a questionnaire, in order to verify whether managers were aligned with the objectives of our study. Interviews were based on the analysis of each tool proposed, in order to understand how the company implements them and, if the tools were implemented, how "attack" security and "supply" security performances are affected by them (by a positive or negative impact). Finally, we have also pointed out the perceived importance that managers have about the proposed tools and about the cause factors which determine a bad security performance. After the first interviews, we noticed that there were some issues for the interviewer in answering our questionnaire, and than, we solve them by putting together all the tool related to "**Awareness development of security with partners**" and "**Reduction of cultural differences between company and partners**" in a unique tool called "**Development of internal awareness about security**" because the fact they did not perceive an effective difference among the tools, and by using the final client delay as the unique KPI for the "supply" security. The results of the 13 interviews we made, allow us to map the as-is situation of implementation of the tools and their impact on the company security performance; in addition it also provide us the database to answer the 5 research questions.

Table 4 summarized the characteristics of target companies.

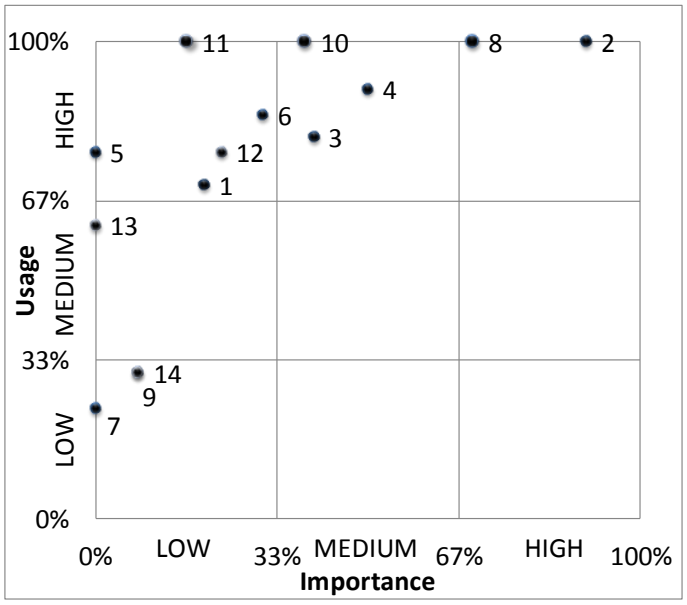
Table 4: Target companies

Companies	Contingency factors					
	Dimension	Scope	Rule	Vertical inegration	Type of goods	Geographical extension
AMBROGIO	Big	Road-rail	MV+GO	high	A	INT
BAS LOGISTICS	Small	road	MV	low	A+P	INT
EWALS INTERMODAL	Big	road	M	low	A+P	INT
FERCAM	Big	road	M	low	A+P	INT
HOYER GROUP	Big	road	MV	low	P	INT
HUPAC	Big	rail	GO	high	A+P	INT
INTERPORTO RIVALTA SCRIVIA	Big	Road-rail	M+G	high	A+P	INT
MARENZANA	Small	road	MV	low	P	INT
MAGAZZINI DESIO BRIANZA	Small	Road-rail	M+G	high	N	INT
SOGEMAR	Big	Road-rail	MV+GO	high	A+P	INT
TI.MO.	Small	rail	G	low	A+P	ITA
TERMINALI ITALIA	Small	rail	G	low	A+P	ITA
VOTG	Big	road	M	high	P	INT
LEGEND:	M = MTO, MV = MTO e road carrier, G = terminal manager, GO = terminal manager and commercial operator, P = dangerous goods, A = desirable goods, N = others					

With regards to the dimensional factor, we took into account the definitions of the European Commission 6 May 2003, n. 2003/361/Ce. In relation to the vertical integration we considered integrated those companies that plays into two roles (road and rail), or, in case they only act in the rail sector, if they are completely integrated in the rail chain (G + GO + rail operator). Accordingly to this classification, we did not considered useful to consider 2 out of 6 contingency factors, due to the low heterogeneity; hence we focus only on dimension, scope, role and vertical integration.

Outcomes of research

Referring to the first research question about which cultural tools are implemented by companies, the analysis related to the whole target highlighted that there are 3 tools less used than others. Figure 8 shows the grafic that distinguish all the proposed tools in term of the usage and the perceived importance by companies.



(1) Multitask working force
(2) Employees cooperation
(3) Integrity and loyalty of employees
(4) Development of internal awareness about security
(5) Soft aspects
(6) Continuous improvement
(7) Business Continuity Planning
(8) Reporting of accident and weakness
(9) Knowledge management
(10) Assessing of security compliance
(11) Partnership
(12) Awareness development of security with partners
(13) Reduction of cultural differences between company and partners
(14) Costumer focus

Figure 8: Usage/Importance – Total

The tools placed in the low usage and low importance quadrant are the following: the "Business continuity planning", probably because his difficulties of implementation in the intermodal sector, the "Knowledge management", easier to implement in human intensive sectors and the "Costumer focus", because to the nature of the intermodal chain (very highly fractionated) and to the lack of an incentive system that could guarantee in all the step of the chain a specific attention to positive results in security. In order to answer the second research question about what impact cultural tools have on security performance, we developed two cause maps to highlight the different impact that the tools have on security KPIs.

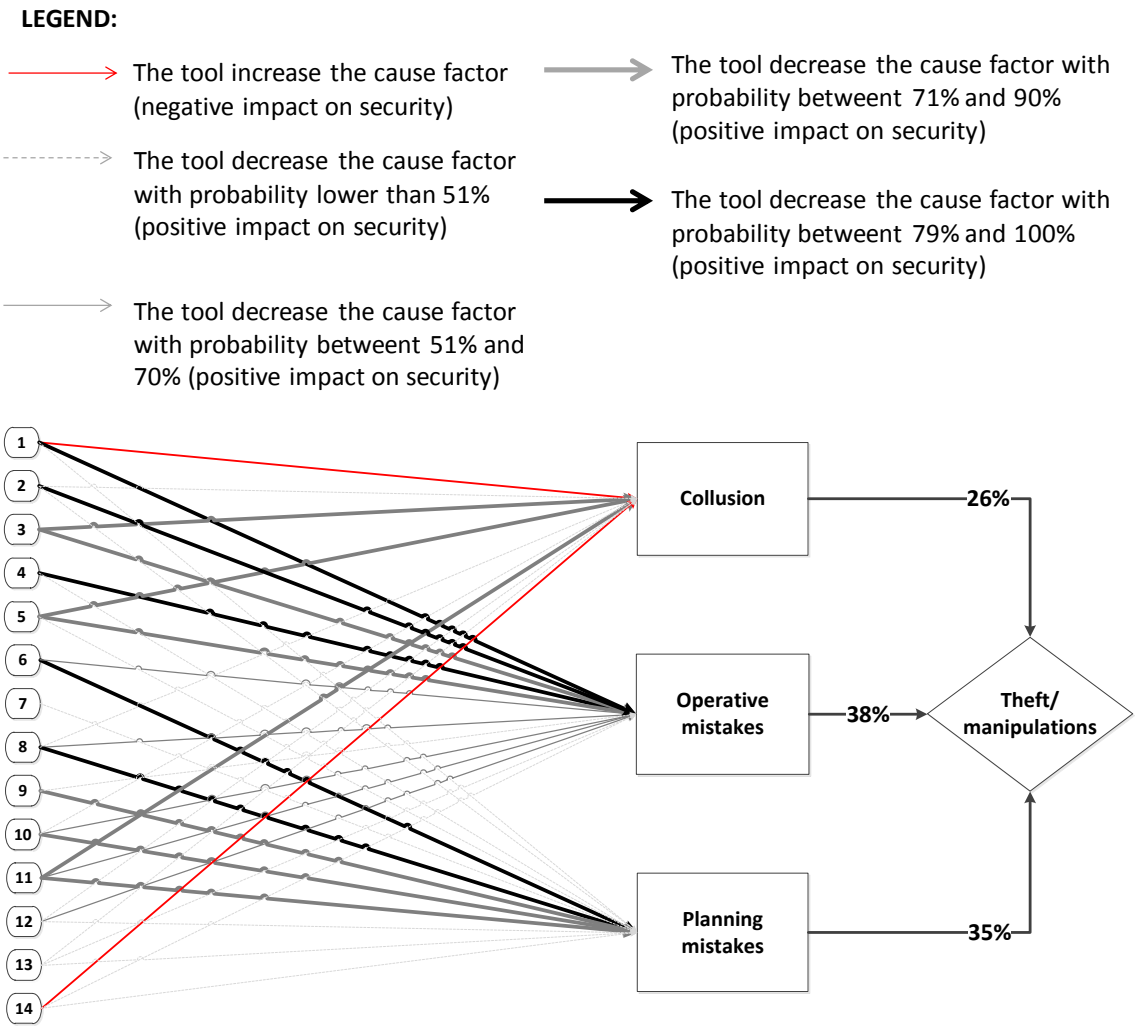


Figure 9: Map-total-scurity "from attacks"

Referring to the map in Figure 9, it is clear that the causes related to thefts or manipulations are balanced. The collusion is slightly less important, in spite of multitask workforce and costumer focus have a negative impact on it. This means that companies are able to manage at best the trade-off caused by these tools on security performance. Despite several tools positively impact on operative mistakes, these since to be the main reasons affecting the "attack" security performance. From interviews is generally raised that companies are well equipped to limit threats and manipulations.

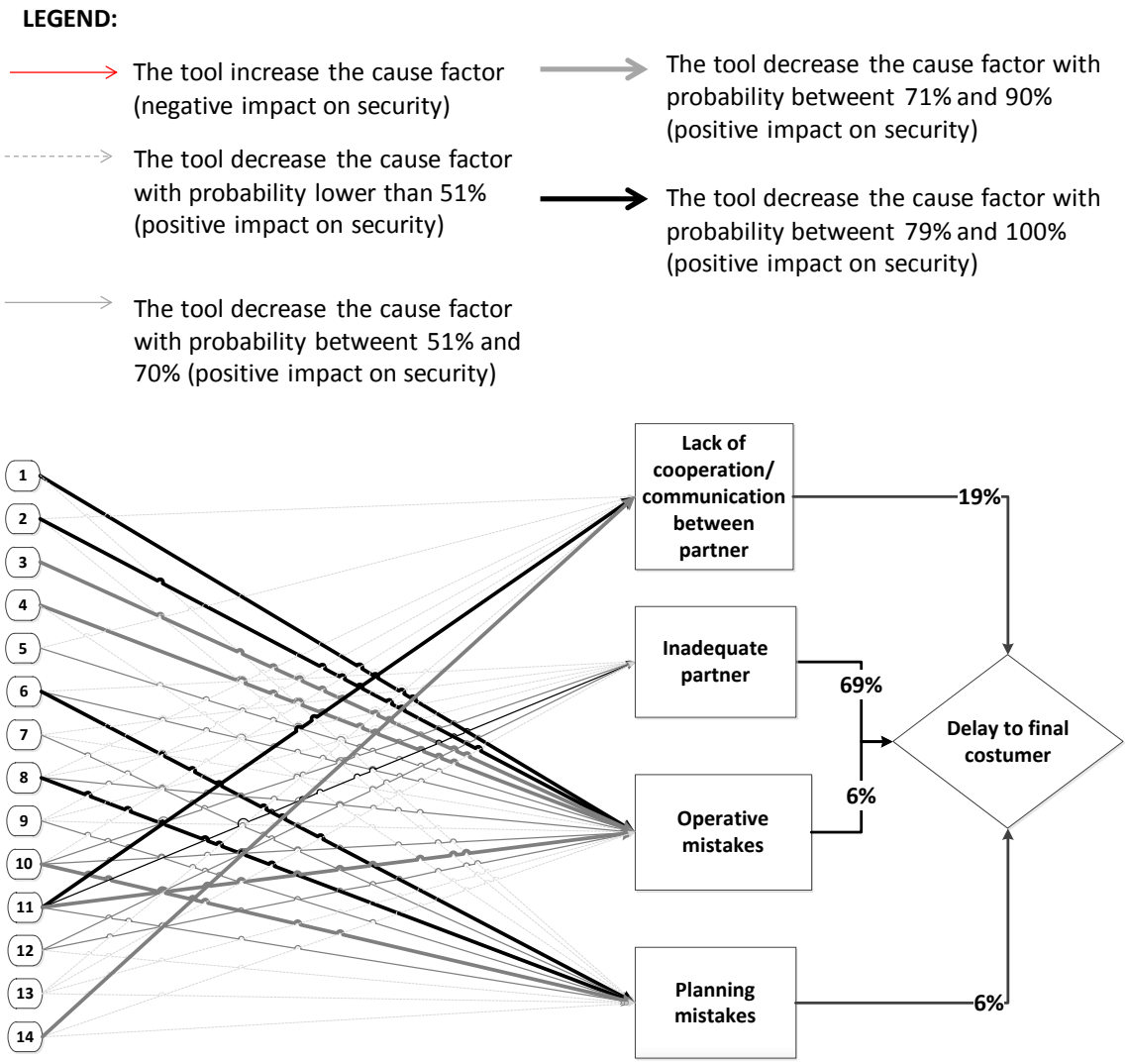


Figure 10: Map-total-scurity "from supply"

Referring to the map in Figure 10, it is clear how the main problem intermodal companies are dealing with is the relationship with partners in the chain. Analyzing the impact of tools, we can see how these are weak on the external causes (lack of cooperation and inadequate partner), and that they are the main responsible to get a bad performance in term of "supply" security. The reason is the different use between internal and external tools: in fact, the first ones are largely used by company that, by historical and cultural behaviors, are forced to focus on internal process and performances. About the use of external tools, there are, on the other hand, some lacks regarding their use, and than this could explain the high impact that external causes have on the final performance.

About other research questions, we conducted the same analysis splitting the company target on the bases of the contingency factors. Final results provide a general overview

about the different use of the proposed cultural tools related to the different contingency factors. As it was assumed, big companies are pushed toward major use and formalizations of tools (intended as standardizations of the way to use). As a result, on average, 11.75 out of 14 proposed tools are implemented by big companies, 9.3 of which formally; instead, the average number of tools implemented by small companies decreases to 8.2, 4.4 of which formally. This fact is due to the high internal complexity of the companies that makes it difficult to achieve the security target without the formal use of the proposed tools. An additional reason for the differences between small and big companies is the fact that a big dimension (with the consequent higher complexity, higher turnover and higher bargaining power), allows big companies to hold an advantaged position by implementing the proposed tools.

With regards to the integration, there isn't a clear difference in the use of the proposed tools. (companies with high integration implement on average about 11 out of 14 tools, 8.4 of which formally, against the 9.57 tools implemented by low integrated companies, about 6 of which formally).

The integration is a discriminant factor only for two tools: multitask workforce (better explained by the scope) and business continuity planning. Moving to the contingency factor scope, we noticed how all the external tools linked to the chain performances are better implemented by company that works in the road sector. In particular, we allude to the tools of awareness development of security with partners, the reduction of cultural differences between company and partners and the customer focus, which are on average implemented by the 72% of the companies with road interface and by the 33% ones with rail interface.

To help thin kind of companies in implementing these tools, is the responsibility of the performance they have in front of the final customer, because the fact companies are closely connected to them. These companies developed the concept to belong to a unique chain and they commit themselves to reduce cultural differences, in order to develop competences and consciousness on security topics, so that being able to reach high target performances. We can also notice another difference between companies playing in different scopes. From one side, companies with rail interface need to employee a multitask workforce due to the high number of operative tasks done within the intermodal terminal (used by 67% of rail companies against the 33% of road ones). On the other side, companies that play in the road scope tend to apply more structured and formal tools linked to the development of security competence (formally used by

100% of road companies against the 33% of rail ones) and the accident reporting (formally used by 83% of road companies against the 33% of rail ones). This trend is supported by the fact that into the road scope it exists an higher variability of risks which can bring to disruption, in comparison to the rail scope.

Beside running analysis that take into account a contingency factor per time, we also run a cross analysis combining all the potential contingency factors, hence getting 8 different clusters. Every company operating in the intermodal sector can then be placed to a specific cluster basing on its specific contingency factors. The results of these cross analysis led to the development of 8 different check-lists of cultural tools (Figure 11 and Figure 12) that allow a generic company to achieve security performances in line with that sector. This does not mean to have optimal security performance, because even if the performance are good for "attack" security, this is not true for the ones of "supply". As it is shown in figure 9, there is a clear difference between intra-company and inter-company cause factors; this difference suggests us that the sector has a good internal security but also some lacks on the external one, hence leaving high margin of improvement regarding the relationships with the chain partners. We think that using the external tools proposed by a structured way – which tools accordingly to the initial analysis on the total target were less utilized and less perceived as important – it is possible to significantly decrease the delay to the final customer, hence achieving a high security performance in term of "supply".

Big Company												
Road						Rail						
high vertical integration			low vertical integration			high vertical integration			low vertical integration		
Check-list tools for cluster A			**Check-list tools for cluster C**			**Check-list tools for cluster E**			**Check-list tools for cluster G**		
Common	2	Employees cooperation	Common	2	Employees cooperation	Common	2	Employees cooperation	Common	2	Employees cooperation
	3	Integrity and loyalty of employees		3	Integrity and loyalty of employees		3	Integrity and loyalty of employees		3	Integrity and loyalty of employees
	5	Soft aspects		5	Soft aspects		5	Soft aspects		5	Soft aspects
	6	Continuous improvement		6	Continuous improvement		6	Continuous improvement		6	Continuous improvement
	8	Reporting of accident and weakness		8	Reporting of accident and weakness		8 (n.f)	Reporting of accident and weakness		8 (n.f.)	Reporting of accident and weakness
	10	Assessing of security compliance		10	Assessing of security compliance		10	Assessing of security compliance		10	Assessing of security compliance
	11	Partnership		11	Partnership		11	Partnership		11	Partnership
Characteristic	**4**	**Development of internal awareness about security**	**Characteristic**	**4**	**Development of internal awareness about security**	**Characteristic**	**1**	**Multitask working force**	**Characteristic**	**1**	**Multitask working force**
	7	**Business continuity planning**		**9 (n.f.)**	**Knowledge management**		**4 (n.f.)**	**Development of internal awareness about security**		**4 (n.f.)**	**Development of internal awareness about security**
	9 (n.f.)	**Knowledge management**		**12**	**Awareness development of security with partners**		**7**	**Business continuity planning**		**9 (n.f.)**	**Knowledge management**
	12	**Awareness development of security with partners**		**13**	**Reduction of cultural differences between company and partners**		**9 (n.f.)**	**Knowledge management**	Unused	7	Business continuity planning
	13	**Reduction of cultural differences between company and partners**		**14 (n.f.)**	**Costumer focus**	Unused	12	Awareness development of security with partners		12	Awareness development of security with partners
	14 (n.f.)	**Costumer focus**	Unused	1	Multitask working force		13	Reduction of cultural differences between company and partners		13	Reduction of cultural differences between company and partners
Unused	1	Multitask working force		7	Business continuity planning		14	Costumer focus		14	Costumer focus

Figure 11: check-list of cultural tools for big companies

Small Company												
Road						Rail						
high vertical integration			low vertical integration			high vertical integration			low vertical integration			
Check-list tools for cluster B			**Check-list tools for cluster D**			**Check-list tools for cluster F**			**Check-list tools for cluster H**			
Common	2 (n.f.)	Employees cooperation	Common	2 (n.f.)	Employees cooperation	Common	2 (n.f.)	Employees cooperation	Common	2 (n.f.)	Employees cooperation	
	3 (n.f.)	Integrity and loyalty of employees		3 (n.f.)	Integrity and loyalty of employees		3 (n.f.)	Integrity and loyalty of employees		3 (n.f.)	Integrity and loyalty of employees	
	5 (n.f.)	Soft aspects		5 (n.f.)	Soft aspects		5 (n.f.)	Soft aspects		5 (n.f.)	Soft aspects	
	6 (n.f.)	Continuous improvement		6 (n.f.)	Continuous improvement		6 (n.f.)	Continuous improvement		6 (n.f.)	Continuous improvement	
	8	Reporting of accident and weakness		8	Reporting of accident and weakness		8 (n.f.)	Reporting of accident and weakness		8 (n.f.)	Reporting of accident and weakness	
	10 (n.f.)	Assessing of security compliance		10 (n.f.)	Assessing of security compliance		10 (n.f.)	Assessing of security compliance		10 (n.f.)	Assessing of security compliance	
	11	Partnership		11	Partnership		11	Partnership		11	Partnership	
Characteristic	**4 (n.f.)**	**Development of internal awareness about security**	**Characteristic**	**4 (n.f.)**	**Development of internal awareness about security**	**Characteristic**	**1 (n.f)**	**Multitask working force**	**Characteristic**	**1 (n.f.)**	**Multitask working force**	
	12 (n.f.)	**Awareness development of security with partners**		**12 (n.f.)**	**Awareness development of security with partners**	Unused	4	Development of internal awareness about security	Unused	4	Development of internal awareness about security	
	13 (n.f.)	**Reduction of cultural differences between company and partners**		**13 (n.f.)**	**Reduction of cultural differences between company and partners**		7	Business continuity planning		7	Business continuity planning	
Unused	1	Multitask working force	Unused	1	Multitask working force		9	Knowledge management		9	Knowledge management	
	7	Business continuity planning		7	Business continuity planning		12	Awareness development of security with partners		12	Awareness development of security with partners	
	9	Knowledge management		9	Knowledge management		13	Reduction of cultural differences between company and partners		13	Reduction of cultural differences between company and partners	
	14	Costumer focus		14	Costumer focus		14	Costumer focus		14	Costumer focus	

Figure 12: check-list of cultural tools for small companies

As a supplement of the ceck-lists, we have also summarized the best practices that were raised during the interviews regarding the application of the suggested cultural tools.
Finally we have summarized the cross topics found out during the interviews regarding the management of the intermodal services and its future developments.
These topics are:

- Role of information. Beside the benefits described in literature there are also potential risks linked to the increasing amount of collusions;
- Benefits of vertical integrations. This is the trend of the major companies playing in the sector that recognized the benefits in term of control and visibility of the end-to-end transport.
- Intermodal service focus. From one side we reported a trend intended to differentiate the offer of intermodal services toward other transport ways, hence moving the attention from a generic price battle to distinctive qualities of intermodal transport. On the other side, came out a trend in focusing on specific routes in order to obtain a better control and a consequent improvement of the transport security.
- Service quality push. Intermodal transport has clear advantages on security, effectiveness and eco-sustainability. The lack of policies that incentive this performances are a big obstacle to the development of the intermodal transport.
- Rail transport perception from companies and public opinion. Here we refer to the Italian situation that considers rail transport as an inefficient and unsure. Actually the issue is partly cultural and partly linked to historical views, and also emphasized by the lack of consistence and a real political commitment for the development of rail transport.

Conclusions and future research

The original contribution of our thesis is the deepening, within the study of SCS, of a less developed area referred to the SCSC. We proposed a structured classification of the tools that support the development of this new approach to security that was not present in literature. The chosen method of analysis is also different from the one used for the classical security tools because, due to the nature of the cultural tools, it's not possible to simply suggest a cost-benefit based relation. Our reference in term of theoretical model that combines qualitative and quantitative information can be further expanded to

every company within the intermodal sector. Through a map of as-is situation it has been possible to find out specific check-lists of cultural tools for each kind of companies; this benchmark is very helpful to aligned the security company performance with those present in the average of the sector. We have also find out improving areas for these performance and the current best practices of the sector. One limitation of the proposed model is the small number of companies in the target which did not allow us to make a robust statistical analysis; moreover we also introduced some approximations on model parameters due to the impossibility to get historical data coming from company database. We also noticed that it is possible to run a further complementary study considering other organizational performances linked to the security one (as it is described in Figure 4).

Finally the study was able to answer in a very detailed way to all the research questions proposed.

1 Il trasporto intermodale

In questo capitolo presentiamo la tematica del trasporto intermodale partendo dalle definizioni formali, passando ai vantaggi teorici per arrivare alle direttive europee a sostegno di questo nuovo approccio al trasporto. Proponiamo diverse tipologie di classificazione circoscrivendo la nostra analisi al trasporto intermodale strada-ferrovia. Evidenziamo inoltre le criticità di questa tipologia di trasporto soffermandoci sulle sue peculiarità in Italia. Viene infine proposta una descrizione delle responsabilità base degli attori all'interno della filiera intermodale strada-ferrovia.

1.1 Premessa

Il trasporto intermodale non è una nuova modalità di trasporto, ma un approccio alla pianificazione dei trasporti con il quale si cerca di sfruttare i vantaggi di ogni sistema di trasporto e ridurre al minimo gli svantaggi derivanti da essi.

Il trasporto intermodale ha cioè l'obiettivo di individuare il sistema di trasporto più indicato per ogni singola tratta in funzione di variabili quali costi, tempi, affidabilità, inquinamento, ecc.

Questo approccio alla pianificazione consente quindi di effettuare un trasporto da un punto di origine ad uno di destino cambiando all'occorrenza modalità di trasporto, passando dalla strada alla ferrovia, dall'aereo al mare in funzione della tratta da percorrere così da sfruttare i vantaggi derivanti da ogni singola modalità di trasporto.

Date le molteplici e diverse definizioni presenti in questo settore, nel 2001 tre organi internazionali, CEE (commissione dell'unione europea), CEMT (conferenza Europea dei ministri dei trasporti) e CEE/NU (commissione economica per l'Europa delle Nazioni Unite), hanno redatto congiuntamente un documento intitolato "Terminology on combined transport" nel quale hanno fornito un glossario comune dei termini normalmente utilizzati. Riportiamo di seguito la classificazione di tre differenti termini.

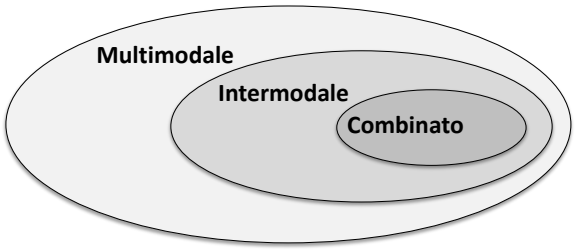


Figura 13: classificazione trasporti multimodali

Trasporto multimodale: *"trasferimento di merce tramite l'utilizzo di almeno due diverse modalità di trasporto".*

Trasporto intermodale: "*trasferimento di merce effettuato mediante più modi di trasporto ma una sola unità di carico, senza rottura del carico stesso, l'unità di carico può essere un veicolo stradale oppure una ILU"* (intermodal load unit: container, cassa mobile, semirimorchio).

Trasporto combinato: "*trasporto intermodale in cui la maggior parte del tragitto si effettua per ferrovia, vie navigabili o mare, mentre i percorsi iniziali e finali, i più corti possibili, sono effettuati su strada".*

Il nostro lavoro di Tesi si svilupperà prendendo in considerazione il trasporto intermodale nel suo complesso (per cui focalizzandoci solo sui trasporti di merce senza rottura di carico), spesso però lo schema di analisi sarà molto vicino al trasporto combinato in quanto è la modalità di operare più comune all'interno del trasporto intermodale; in particolare il nostro focus sarà sul trasporto combinato strada-ferrovia.

1.2 Vantaggi

Come spiegato da Mazzarino (1998) esiste un intervallo ottimo del rapporto distanza-peso per ciascuna modalità di trasporto. Egli afferma infatti che *"si deve utilizzare il trasporto più adatto sulle diverse classi di distanza e per i diversi pesi trasportati"* così da massimizzare l'efficienza del trasporto, tramite il raggiungimento delle economie di scala associate a ciascuna modalità di trasporto. Un semplice esempio di come si può applicare questo concetto sulla dimensione distanza è illustrato nel seguente grafico dove si è costruita la curva di costo di ciascuna modalità tenendo conto dei costi fissi (CF sulle ordinate, riferiti ai mezzi di trasporto e alle attrezzature) e dei costi variabili (dati dalle pendenze delle rette, riferiti al personale, carburante, pedaggi in funzione dei km percorsi), sostenuti da chi effettua fisicamente il trasporto.

Tramite la Figura 14 si nota immediatamente la convenienza nel cambiare modalità di trasporto in corrispondenza dei punti 1 (al di sopra della quale il trasporto su rotaia risulta più conveniente di quello su gomma), 2 (nel quale il miglior trasporto possibile rimane quello su rotaia, mentre i costi legati al trasporto su gomma superano quelli legati al trasporto marittimo), 3 (al di sopra del quale il trasporto marittimo diviene quello in assoluto più efficiente).

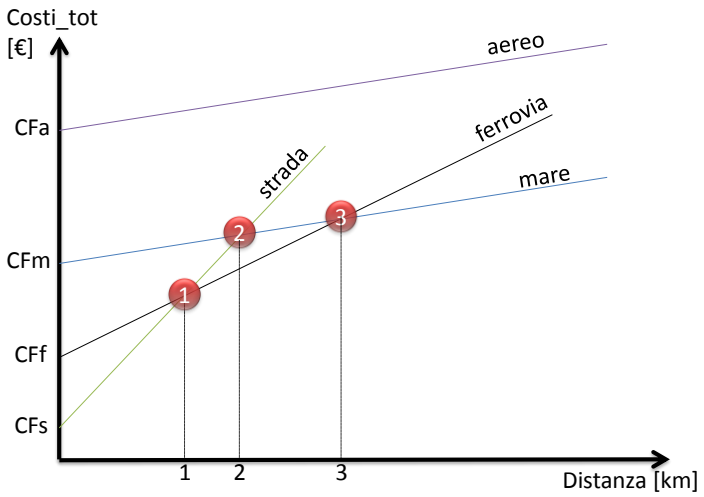


Figura 14: grafico dei costi delle varie modalità di trasporto in funzione della distanza

Questa modellizzazione è in accordo con Quattroccolo (2011) che, in riferimento al trasporto intermodale strada-ferrovia, sostiene: *"al variare di parametri quali il volume di traffico da soddisfare o la densità degli insediamenti da servire, il rapporto fra i valori di costo globale del trasporto riferiti alle modalità su strada e su rotaia si modifica fino ad invertirsi"*.

Il trasporto intermodale consente quindi di sfruttare a pieno queste considerazioni economiche, compatibilmente ai vincoli naturali ed infrastrutturali, così da rendere il trasporto il più efficiente possibile.

In generale la scelta di utilizzare il trasporto intermodale è realizzabile solo quando i benefici derivanti dall'utilizzare in modo integrato le varie modalità di trasporto sono maggiori dei costi connessi.

I benefici in questione sono:

- realizzazione di economie di scala attraverso l'uso ottimale (per dimensione e distanza) di ciascuna modalità e, quindi, riduzione dei costi;
- utilizzo del mezzo di trasporto più idoneo alle caratteristiche del servizio di trasporto (volume, stagionalità e tipologia della merce) per ogni tratta del percorso e, quindi, riduzione dei costi-opportunità;
- incentivi europei e nazionali e minori restrizioni da rispettare (come ad esempio il limite di ore di guida per gli autisti);

- sgombero delle principali arterie stradali con conseguente riduzione degli incidenti stradali.

I costi connessi sono invece:

- costi delle operazioni terminali;
- costi di organizzazione;
- costi legati all'utilizzo di unità di carico standardizzate;
- aumento dei tempi di viaggio;
- probabile minor qualità del servizio (in termini di minor affidabilità, flessibilità e controllo).

Oltre a considerazioni di tipo economico, in questi ultimi anni, il trasporto intermodale si è sviluppato grazie alla maggior attenzione per la sostenibilità ambientale. Adottare infatti un approccio intermodale, favorendo ad esempio il trasporto ferroviario rispetto al trasporto cosiddetto "tutto strada", consente un dispendio minore di energia unito ad un minore inquinamento, come testimonia la Tabella 5.

Tabella 5: dati riferiti ad un trasporto di 900 tonnellate da Verona a Lubecca. (Fonte: EcoTransit UIC-Ifeu)

	Consumi di Energia [GigaJoule]	Emissioni gas serra [tonnellate CO2]
Camion	1.215	81
Treno	517	27
	-57%	-67%

1.3 Direttive europee

Proprio a seguito di considerazioni ambientali di questo tipo, l'Unione Europea ha intrapreso negli anni una serie di programmi in favore dell'intermodalità, tra i quali i Libri bianchi e il programma MARCO POLO.

Libri Bianchi[4]

Con i tre Libri bianchi (1992, 2001, 2011) redatti dall'UE in favore della sostenibilità nei trasporti, sono state sostenute iniziative atte a promuovere la costruzione delle grandi reti trans europee e diversificare i servizi di trasporto, così da ridurre gli squilibri tra le varie modalità di trasporto.

4 Scritto utilizzando le informazioni incluse nel Libro Bianco (2011)

Le politiche di riforma, ad oggi, non sono riuscite a cambiare in modo strutturale il sistema della mobilità, infatti è ancora lontano il bilanciamento di utilizzo delle diverse modalità di trasporto (come richiesto dal Libro bianco del 2001). Il sistema è rimasto fortemente legato al trasporto su strada e a mezzi "non sostenibili" dal punto di vista ambientale e delle risorse: la Commissione stima che, all'interno dell'UE oggi, il petrolio copra il 96% del fabbisogno energetico per i trasporti, e le emissioni di gas serra derivanti dal settore sono aumentate del 38% (dato 2008) rispetto ai livelli del 1990. In particolare, la Commissione ha rilevato che, nel 2008, le emissioni di gas a effetto serra derivanti dal settore trasporti provenivano per il 71,3% dal trasporto stradale, per il 13,5% dai trasporti marittimi, per il 12,8% dai trasporti aerei e per lo 0,7% dai trasporti ferroviari.

Per questo motivo gli sforzi dell'UE si sono orientati verso un ripensamento delle attuali modalità di trasporto. Il Libro bianco 2011 spinge verso modalità di trasporto sostenibili, incentivando l'uso di mezzi "puliti", con l'obiettivo di ridurre entro il 2050 le emissioni di gas serra derivanti dal settore trasporti del 60% rispetto ai livelli del 1990. In linea con l'iniziativa "Un'Europa efficiente sotto il profilo delle risorse", e con il nuovo "Piano di efficienza energetica 2011", all'interno del Libro bianco 2011 vengono delineati dieci obiettivi per modificare le modalità operative di trasporto.

Il discorso è strettamente collegato all'intermodale quando si affrontano le tematiche del trasporto merci sulle lunghe distanze, infatti la Commissione ritiene importante promuovere quei cambiamenti strutturali che consentirebbero al trasporto ferroviario e via acqua di competere con il trasporto merci su strada. L'obiettivo è che sulle percorrenze superiori a 300 km, il 30% del trasporto di merci su strada dovrebbe essere trasferito entro il 2030 verso altre modalità, quali la ferrovia o le vie navigabili. Nel 2050 si dovrebbe passare al 50% (obiettivo n°3 del Libro bianco).

La Commissione evidenzia che tale "riequilibrio" necessita di connessioni efficienti tra le diverse modalità di trasporto (porti, aeroporti, ferrovie e vie navigabili interne)". Viene quindi delineato un ulteriore obiettivo: "collegare entro il 2050 tutti i principali aeroporti e porti marittimi alla rete ferroviaria e, laddove possibile, alle vie navigabili interne (obiettivo n°6 del Libro bianco).

Un simile riassetto multimodale del trasporto dovrà svilupparsi necessariamente a livello continentale. Per questo motivo la Commissione sottolinea l'importanza di sostenere le reti di trasporto transeuropee (Trans-European Networks - Transport, TEN-T).

L'obiettivo è costruire, entro il 2030, una "rete essenziale" TEN-T multimodale pienamente operativa in tutta l'Unione europea, e nel 2050 una rete di qualità e capacità elevate con una serie di servizi di informazione connessi (obiettivo n°5 del Libro bianco).

Viene inoltre sostenuta la creazione, all'interno della "rete essenziale", di strutture per i corridoi multimodali (Figura 15), atte a sostenere il trasporto a carro completo e la connessione con le vie navigabili interne.

Figura 15: rappresentazione dei 10 corridoi multimodali europei

La Commissione osserva che, oltre allo sviluppo infrastrutturale, l'Unione dovrebbe riuscire ad unificare il mercato interno dei trasporti, in particolare per quanto riguarda i servizi ferroviari e il trasporto di merci su strada.

Tra le iniziative principali indicate nella "Strategia" della Commissione vi è, infatti, quella di sostenere il mercato interno deiservizi ferroviari, attraverso, ad esempio, l'aggiudicazione obbligatoriadi appalti pubblici mediante procedure di gara, un'autorizzazione unica dei tipi di veicolo ed un'unica certificazione di sicurezza dell'impresa ferroviaria, garantendo così l'accesso non discriminato alle infrastrutture e ai servizi.

Per quanto riguarda invece il mercato interno del trasporto merci su strada, la Commissione si impegna a modificare la legislazione in materia di pesi e dimensioni così da rendere più agevole il trasporto intermodale e ridurre il consumo globale di energia e le emissioni.

Il programma Marco Polo II

Il programma Marco Polo II ha come fine ultimo la riduzione della congestione delle infrastrutture stradali e il miglioramento delle prestazioni ambientali dell'intero sistema di trasporto. Per poter raggiungere questo scopo, il programma sostiene il trasferimento del traffico merci dalla strada verso la navigazione marittima a corto raggio, la ferrovia e la navigazione interna. Ciò rappresenta 12 miliardi di tonnellate-kilometro l'anno[5].

Attuato successivamente al programma PACT (Pilot Action for Combined Trasport, 1997-2001) e Marco Polo (2001-2007), con il quale condivide gli obiettivi di fondo, Marco Polo II sovvenziona azioni commerciali sul mercato del trasporto merci a cui partecipano almeno due Stati membri dell'UE.

Il programma è incentrato esclusivamente sulla promozione di servizi commerciali sul mercato del trasporto merci e non riguarda né ricerca e sviluppo né le misure a favore delle infrastrutture.

1.4 Classificazione[6]

Esistono numerose classificazioni del trasporto intermodale; la più immediata è quella in base alle modalità di trasporto utilizzate. Esse possono essere di cinque tipologie:

- per mare tramite nave;
- per via fluviale tramite chiatte;
- tramite aereo;

5 Dato estrapolato dal Programma Marco Polo II (24 novembre 2011)

6 Capitolo scritto in collaborazione con l'Ing. Fulvio Quattroccolo fondatore e gestore del sito web www.intermodale24-rail.net

- via ferrovia;
- via strada.

Queste modalità possono essere combinate a due a due, oppure utilizzate anche tre, quattro o al limite tutte per un singolo trasporto intermodale dando vita così a numerose tipologie di trasporto intermodale.

Nella nostra trattazione analizzeremo il trasporto combinato strada-rotaia, per cui da ora in avanti faremo implicitamente riferimento allo schema logico in Figura 16.

Nella Figura 16 si notano tutti i passaggi che la ILU deve effettuare durante il trasporto intermodale strada-ferrovia; dal punto di origine a quello di destino passando dal trasportatore su gomma, al trasbordo nel terminal intermodale e alla trazione ferroviaria.

Figura 16: schema di processo del trasporto combinato strada-rotaia

Entrando nel merito del trasporto su rotaia si evidenzia la possibilità di un'ulteriore classificazione in funzione della diversa gestione del servizio ferroviario, in particolare si distinguono i seguenti casi:

- trasporto a treno completo
  - diretto
  - shuttle
  - sistema gateway
- trasporto a treno a carico singolo

Treni completi

Questi treni circolano nella rete del combinato europeo che collega tra di loro i terminal e i porti europei. Sono detti punto a punto in quanto viaggiano da origine a destino senza soste intermedie. Lungo questa rete i treni possono viaggiare con velocità più elevate, normalmente 120 km/h (in Italia 100 km/h), pertanto vengono garantiti tempi di resa migliori. Ormai a livello europeo dell'80-90% del traffico combinato viaggia con questa modalità di trasporto, entrando nello specifico, si divide in:

***Treni diretti*:** si tratta di treni che partono da una specifica origine e raggiungono un'unica destinazione; vengono composti in funzione della destinazione e del volume di merce. Per essere economicamente vantaggiosi devono raggiungere livelli di saturazione molto elevati in quanto, nella maggior parte dei casi, effettuano il ritorno a vuoto. Per giustificare il loro utilizzo sono necessari perciò elevati volumi nella tratta di andata. Solitamente viaggiano di notte, in modo da raggiungere la stazione di destinazione nelle prime ore del mattino del giorno seguente a quello di partenza.

Figura 17: schema di processo del sistema a treno diretto

Treni shuttle: si tratta di treni diretti per i quali è stato creato un vero e proprio servizio di linea per il trasporto merci. Individuati due terminal con alti volumi di traffico, questi vengono di volta in volta collegati fra loro da treni a composizione fissa che partono anche più volte al giorno secondo orari prestabiliti. In presenza di relazioni stabili, questa soluzione è ancora più efficiente rispetto ai treni completi, poiché si mette a disposizione la capacità di un intero treno sia per il viaggio di andata che per il ritorno (il treno parte indipendentemente dal fatto che sia stato riempito o meno). Si hanno così vantaggi in termini di velocità, programmabilità, efficienza (ad esempio basta una sola lettera di vettura per l'intero treno e i controlli alla frontiera non vengono effettuati) ma anche di sicurezza (evitando tutte le operazioni di smistamento è adatto per merci delicate o pericolose). All'interno del panorama italiano alcuni esempi di collegamenti shuttle open-access partono dai terminal di Mortara (organizzati da Shuttlewise), di Busto (organizzati da Hupac S.p.A.), da Melzo (ERS Railways) e Verona Quadrante Europa (organizzati da Hupac e Kombiverkehr) o si tratta di company train come quelli di Ambrogio S.p.A. (che ha volumi tali da gestire 2 o 3 treni al giorno), o di grandi clienti come il Gruppo Arcese S.p.A. (che si appoggia ad Hupac).

Figura 18: schema di processo del sistema shuttle

I treni diretti e i treni shuttle sono detti "Punto a punto", in quanto viaggiano da un punto di origine ad uno di destino senza soste intermedie.

Sistema gateway: è un sistema del tipo "hub and spoke", i treni hanno come destinazione uno scalo di smistamento in cui i vagoni vengono a loro volta manovrati per costituire dei nuovi treni con una precisa destinazione. All'interno dello scalo dove questi treni vengono manovrati viene dedicata una sezione ad "hoc" così da permettere che i tempi di resa siano di buon livello e decisamente migliori rispetto al traffico diffuso. Questo tipo di trasporto rappresenta uno stadio intermedio tra il traffico diffuso e i treni completi, infatti la prima tratta può essere effettuata tramite un carico singolo o un treno diretto mentre la seconda tramite un sistema shuttle. Esempi italiani sono il gateway di Busto (gestito da Hupac S.p.A.) dove arrivano flussi dal nord Europa e vengono smistati a Milano, Padova e Bologna, quello di Melzo in cui sono presenti rilanci per Nola e il gateway di Novara che ha rilanci per Bari e Pomezia. Solitamente in Italia sono le sole unità di carico che vengono trasbordate su nuovi treni per essere rilanciate verso altre destinazioni; è più raro invece che un'intera sezione di treno venga fatta proseguire su altri scali.

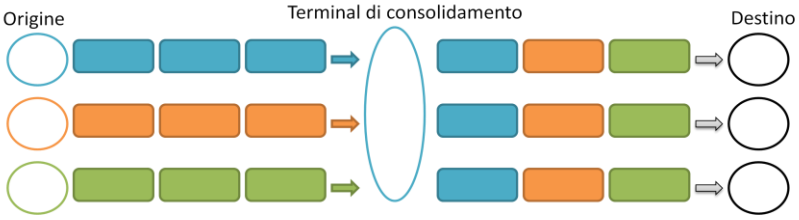


Figura 19: schema di processo del sistema gateway

Treni a carico singolo

Nell'ambito del trasporto combinato le unità vengono spedite anche con vagoni singoli, che solitamente giungono a destinazione in alcuni giorni a seconda delle località richieste poiché viaggiano nei treni del reticolo del diffuso. Questo trasporto ferroviario viene utilizzato soprattutto se i quantitativi tra i due nodi non sono sufficienti per effettuare treni completi; offrono quindi flessibilità a scapito di prestazioni come tempo e prezzo. A livello europeo la percentuale di traffico diffuso rappresenta una quota marginale di circa il 5% del traffico combinato.

La scelta del tipo di servizio ferroviario ottimale dipende quindi da dimensioni quali: volumi da trasportare sia in andata che in ritorno, stabilità degli scambi e quindi rischio di non saturazione dei treni, tipologia della merce, tempo di consegna richiesto.

Tipologia di ILU utilizzata

Per quanto riguarda le Intermodal Loading Unit (ILU) ricordiamo la classificazione di Daschkovska (2010) in:

- ISO container
  - general container: per merce standard, senza nessuna particolare esigenza;
  - bulk container: utilizzati per il carico di merce sfusa;
  - named cargo container: DIN EN ISO del gennaio 1996 ha specificato sotto la lettera S alcune tipologie di container per trasportare ad esempio rocce (S0), automobili (S1), pesce vivo (S2);
  - thermal container: per prodotti refrigerati o da riscaldare;
  - open-top container: con tetto apribile o rimovibile indicato per merce molto pesante, spesso sono coperti da particolari teloni;
  - tank container (Figura 20): utilizzati per il trasporto di merce liquida o gassosa;

Figura 20: tank container adibito al trasporto di merce liquida o gassosa

- Casse mobili e non-ISO container: nati dall'esigenza di trovare un imballaggio secondario in grado di raggiungere una saturazione migliore di quella che si può ottenere usando gli ISO container (con un container da 20 piedi si raggiunge un livello di saturazione pari a 77% mentre con uno da 40 piedi 85%), le casse mobili vengono utilizzate soltanto nel trasporto strada-rotaia e generalmente non sono rinforzate e quindi non sovrapponibili.

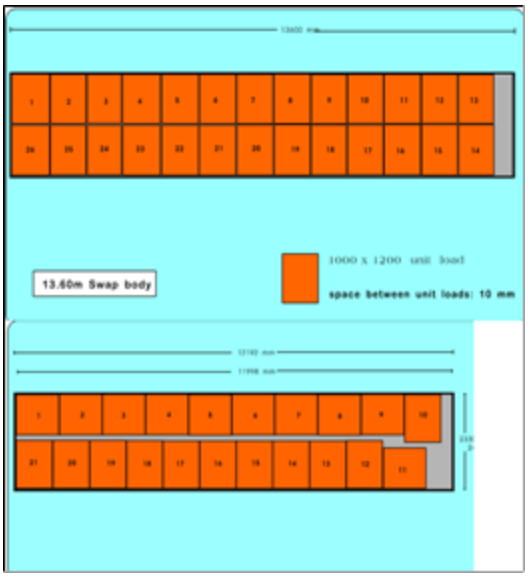


Figura 21: differenza di saturazione superficiale in base all'utilizzo di casse mobili o semirimorchi (97%) e di ISO container da 40 piedi (85%)

- Semirimorchi: veicolo destinato ad esser accoppiato ad un altro motorizzato sul quale si appoggia, ma su cui non scarica la maggior parte del peso che invece è sostenuto dal veicolo stesso; i semirimorchi devono essere attrezzati per poter essere adeguati al trasporto combinato.

Figura 22: semirimorchio attrezzato con apposite tasche laterali che permettono alle gru di agganciarlo e caricarlo sul carro ferroviario ribassato

Sistema di trasporto accompagnato

Un'ulteriore differenzazione per il trasporto combinato strada-ferro è tra il sistema accompagnato o non accompagnato.

Ad oggi, il sistema di trasporto accompagnato è assimilabile alla cosiddetta "autostrada viaggiante"; ovvero il vettore stradale, comprensivo di rimorchio e motrice, sale

direttamente sul carro ferroviario e l'autista viaggerà anch'esso sul treno in speciali carrozze di accompagnamento (da qui la terminologia trasporto accompagnato).

Il sistema accompagnato più diffuso, sia in Svizzera che in Austria, è quello a carico lineare. Come si può notare dalla Figura 23, i camion (motrice e semirimorchio) possono salire su particolari carri ferroviari ultrabassi percorrendo tutta la lunghezza del treno in modo autonomo, senza la necessità di nessuna attrezzatura particolare. Questo sistema presenta però due svantaggi importanti: gli alti tempi di carico/scarico e, siccome sono predisposti per trasportare oltre al semirimorchio anche la motrice, hanno una percentuale di sfruttamento della portata molto inferiore alla media; infatti la motrice sottrae peso e spazio alla merce (Figura 24).

Figura 23: caricamento del rimorchio e della motrice

Figura 24: autostrada viaggiante in movimento

Esiste un'ulteriore modalità di trasporto accompagnato denominato Modalohor; per questa tipologia di trasporto sono necessari speciali carri ferroviari che, come mostrato in Figura 26 e Figura 25, sono composti da due piattaforme sovrapposte, di cui una rotante che consente al vettore stradale di poter salire sul carro e sganciare la motrice così da poter trasportare solo il rimorchio. Questa modalità di carico/scarico è estremamente economica e rapida: a livello teorico si potrebbe caricare un treno di lunghezza indefinita in pochi minuti, il tempo di carico dell'intero treno corrisponde al tempo necessario ad un camion di salire sulla piattaforma rotante e a quest'ultima di allinearsi con il carro.

Figura 26: carro rotante per il carico orizzontale del vettore stradale

Figura 25: processo di caricamento orizzontale del treno

Nonostante questo consistente vantaggio, il sistema di trasporto Modalohor non è affatto diffuso (tralasciando la realtà francese dove esistono elevati incentivi a sostegno di questa modalità); tra i motivi vi è il fatto che i carri ferroviari necessari sono molto più pesanti e costosi dei carri standard (sia in termini di valore di acquisto che di costi di manutenzione) e richiedono un'attrezzatura particolare per il servizio.

Sistema di trasporto non accompagnato

Con il sistema di trasporto non accompagnato si possono trasportare semirimorchi, casse mobili, container senza la motrice. Questa tipologia di trasporto è la più diffusa ed è considerata la vera alternativa al trasporto su gomma. Per poter caricare/scaricare sui carri ferroviari solo le unità di carico c'è la necessità di utilizzo, nel terminal ferroviario, di particolari gru. Queste possono essere:

- a portale (Figura 27) molto più performanti in termini di tempi e costi (minori spazi di manovra) ma più costose per quanto riguarda l'investimento iniziale;
- gommate (Figura 28) le quali sono più flessibili in quanto non fisse ma più lente e hanno la necessità di più spazio per poter operare.

Figura 28: gru gommata mentre solleva un container

Figura 27: gru a portale

Tabella 6: tabella riassuntiva delle differenze in funzione della modalità di trasporto eseguita

	Traffico combinato accompagnato	Traffico combinato non accompagnato
Unità di carico	• Autocarri • Autotreni • Autoarticolati	• Casse mobili • Semirimorchi • Container
Carri ferroviari	• Carri ultrabassi	• Carri aperti
Modalità di carico-scarico	• Orizzontale	• Verticale

1.5 Criticità in Italia[7]

La situazione italiana del trasporto intermodale ferroviario è fortemente correlata agli incentivi statali; infatti da 5/6 anni a questa parte il traffico intermodale interno ha arrestato il suo sviluppo in concomitanza con una riduzione degli incentivi. Il traffico intermodale interno italiano si limita ai porti (principalmente di Genova e La Spezia), a qualche rilancio di traffico proveniente dal nord Europa (ad esempio i flussi che arrivano a Milano o Padova per proseguire verso Pomezia o Marcianise) oltre alle poche e residue relazioni interne. Più sviluppata è la linea nord padana che riceve i flussi ferroviari provenienti dal nord Europa ma rilancia solo una piccola parte di questi tramite treno (spesso i treni si fermano e inizia la tratta stradale per raggiungere il sud Italia). Paradossalmente è più conveniente in termini di costo e tempo far arrivare la merce a Milano tramite il porto di Rotterdam che non quello di Genova; infatti, nonostante una settimana di viaggio su nave in più, a Rotterdam il processo di sdoganamento è molto più breve in confronto ai circa 20 giorni necessari a Genova. Per questo motivo a Genova sono in atto progetti per sveltire le procedure di sdoganamento con il supporto di terminal come quello di Rivalta Scrivia.

Svizzera e Austria in particolare, ma anche Germania, hanno servizi ferroviari di gran lunga migliori rispetto a quelli italiani; questo perché, oltre ad avere piccole ed efficienti ferrovie locali, hanno un'attenzione al territorio ed una cultura intrinseca che ha permesso un forte sviluppo della ferrovia; infatti se in Italia si inizia a considerare il

7 Capitolo scritto in collaborazione con l'Ing. Fulvio Quattroccolo fondatore e gestore del sito web www.intermodale24-rail.net

trasporto intermodale a partire da una distanza minima di circa 400 km, in paesi come la Svizzera esistono trasporti intermodali interni anche per 100 km. Questa situazione è stata raggiunta anche grazie ai forti disincentivi economici e legislativi applicati nell'ambito del trasporto stradale (ad esempio in Svizzera i camion non possono circolare di notte). In Italia invece spesso le normative sul trasporto stradale non vengono rispettate (ad esempio il numero di ore massime che un'autista può impiegare alla guida) mentre la presenza di una lobby stradale nata negli anni '50, che è in grado di ottenere molta attenzione in ambito politico, ostacola possibili sviluppi della ferrovia, la quale migliora per piccoli passi cercando di non intaccare il business dei trasporti su gomma. Inoltre gli operatori ferroviari incontrano anche difficoltà ad accedere alla rete per inefficienze da parte di Ferrovie dello Stato che è monopolista per quanto riguarda la gestione dell'infrastruttura ed ex monopolista (ma monopolista di fatto) per la trazione su alcune tracce specifiche.

Nonostante i molteplici vantaggi teorici, il trasporto intermodale ferroviario presenta quindi diverse criticità pratiche che ne ostacolano la piena concorrenza con il "tutto strada".

Le criticità in questione possono essere classificate in 4 tipologie:

1. infrastrutturale;
2. gestionale;
3. giuridica;
4. assenza di una chiara divisione dei ruoli.

La prima criticità è di natura infrastrutturale: anche se esistono programmi internazionali di intervento all'infrastruttura ferroviaria, ad oggi la rete è insufficiente. Questa criticità comprende sia l'assenza di interconnessioni fra le reti (tratti infrastrutturali mancanti) sia le differenze nella sagoma limite all'interno della rete ferroviaria. L'Italia in questo è un caso esemplare avendo una rete ferroviaria molto vecchia e con differenze sostanziali riguardo alle limitazioni delle altezze massime. Infatti vi è una discrepanza netta tra l'estremo nord e il resto d'Italia: dall'alto padana in su i profili ammessi sono in linea con quelli del nord Europa (i tratti ferroviari dal Brennero e dal Sempione fino a Novara e Gallarate sono attrezzati per gestire container high cube senza carri ribassati e semirimorchi); mentre già a partire dalla bassa padana la sagoma limite diminuisce fortemente e diviene indispensabile utilizzare carri ribassati per il trasporto di high cube mentre non è possibile caricare i semirimorchi oggi più diffusi. Questo è un grosso problema in quanto i carri ribassati sono poco diffusi e

laddove sono disponibili hanno costi molto elevati in termini di acquisto e manutenzione.

La seconda criticità deriva dal fatto che, all'interno della filiera intermodale, esistono numerosi attori che svolgono molte operazioni diverse: trasporto iniziale e finale su gomma garantendo un certo livello di servizio, trasbordo del carico, organizzazione del trasporto ferroviario trovando carichi di ritorno per non effettuarlo a vuoto. Quest'ultima attività è un forte problema per il trasporto ferroviario in quanto vi è meno flessibilità rispetto al trasporto su strada (si rimane vincolati alla posizione della stazione, mentre con il vettore stradale si può andare a prendere il carico deviando dal percorso prestabilito). Questo implica un forte aumento dei costi che frena di molto la diffusione dell'intermodalità. Un ulteriore criticità gestionale, legata però alla rete ferroviaria, è l'inosservanza della programmazione dei treni (ritardi) strettamente collegata alla mancanza di flessibilità della rete. Questo deriva da due problemi: le lacune fisiche dell'infrastruttura citate in precedenza (in Italia i treni passeggeri hanno la precedenza sui treni merce i quali spesso devono attendere per ore) e piccoli accorgimenti che, come accade in Germania, garantirebbero una fluidità maggiore nella circolazione. Alcuni esempi di questi accorgimenti sono scambi di binari senza dover rallentare, invio di treni a distanza più ravvicinata del normale tenendo conto della loro velocità relativa e aggiornamento real-time della traccia da seguire in caso di particolari problemi. Da parte delle società di trazione viene invece a mancare un controllo continuativo sulla posizione del treno; le uniche informazioni che vengono inoltrate al cliente sono aggiornamenti puntuali sull'avanzamento del treno (treno partito, transito da alcuni punti, treno arrivato). Questa lacuna incide molto nella scelta tra intermodale o "tutto strada" in quanto per le aziende è molto importante avere tracciabilità, soprattutto per merce ad alto valore.

La terza criticità è quella che riguarda il differente stato di attuazione delle direttive europee tra i membri dell'Unione, come la liberalizzazione del mercato ferroviario (che dovrebbe eliminare lo stato di monopolio presente in alcuni stati). In questa confusa fase di transizione, gli ex-monopolisti (come Trenitalia Cargo in Italia) sono i soli ad avere i certificati di sicurezza su tutta la rete, quindi su alcune tratte hanno il monopolio. Essi cercano così di sfruttare questa posizione facendo in modo che il cliente (chi richiede di effettuare un nuovo treno) si affidi a loro per la totalità del trasporto: non solo quindi per la tratta monopolizzata ma anche su quelle dove c'è concorrenza. Questo, naturalmente, porta ad avere un prezzo del trasporto più alto. Un problema

aggiuntivo è relativo al fatto che ci sono delle incompatibilità commerciali fra alcuni operatori (in genere sono gli ex-monopolisti che faticano a collaborare tra loro) e questo a volte rende difficile l'organizzazione stessa di un servizio effettuato su tracce internazionali.

Un'ulteriore tipologia di criticità riguarda l'assenza di una chiara divisione dei ruoli tra gli attori del trasporto intermodale strada-ferrovia. In particolare si fa riferimento al ruolo dominante di alcune imprese che sono contemporaneamente principali azioniste degli operatori commerciali logistici e principali fornitrici di trazione ferroviaria delle stesse (le quali sono membri dell'UIRR[8] e fornitrici di vagoni e servizi ai terminal che a loro volta partecipano in aziende di spedizione e in loro concorrenti). Un caso esemplare è quello di Hupac S.p.A. che fa parte dell'UIRR ed è un operatore commerciale logistico controllato per il 72% da aziende di logistica e trasporto e per il 28% da società ferroviarie e, oltre ad avere partecipazioni reciproche con la concorrente Cemat S.p.A., detiene il 25% di SBB e il 25% di Cross Rail, società di trazione che dovrebbero essere indipendenti per garantire parità di trattamento a tutti i clienti. Questa situazione potrebbe comportare interferenze sull'operatività quotidiana (favoreggiamento della partecipata) limitando di fatto lo sviluppo del trasporto intermodale.

1.6 Attori della filiera

Intervistando sul campo le varie aziende che si occupano di trasporto combinato strada-ferrovia abbiamo individuato (Figura 29) i vari attori che partecipano all'intera filiera.

8 Uion Internationale des sociétés de tran sport combiné Rail-Route

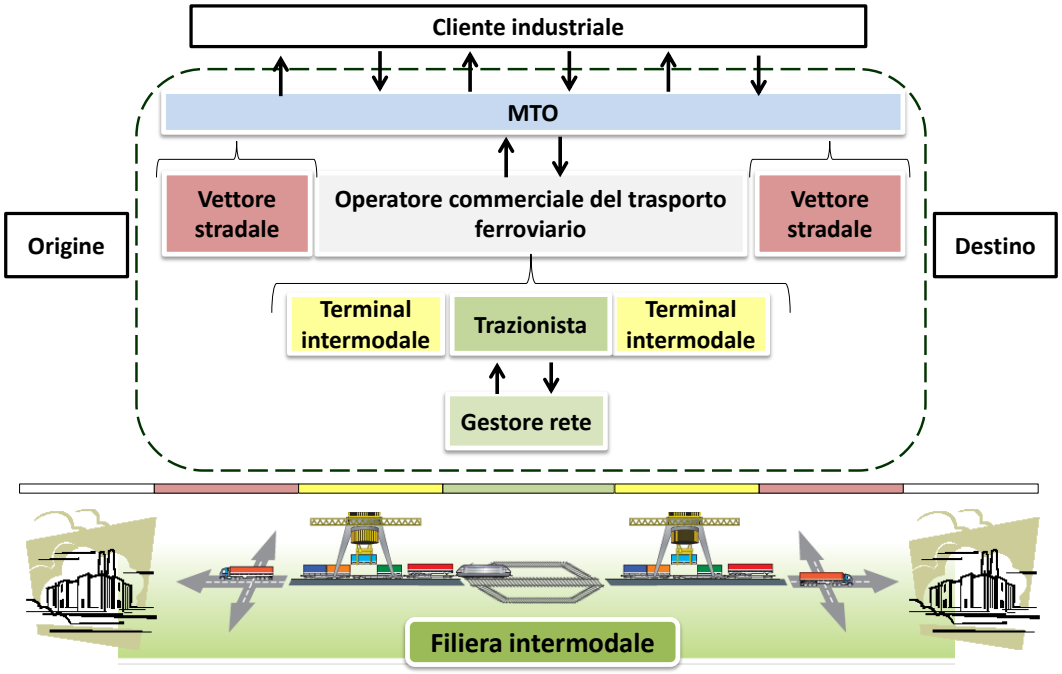


Figura 29: classificazione dei vari attori della filiera intermodale strada-ferrovia

In Figura 29 le frecce indicano uno scambio reciproco di informazioni, mentre le parentesi graffe indicano una pianificazione a livello più alto che deve essere rispettata a livello operativo.

Gli attori evidenziati esprimono i ruoli a livello più atomico di tutta la filiera intermodale e svolgono le seguenti attività:

- cliente industriale: chi ha la necessità di trasportare della merce, solitamente è colui a richiedere esplicitamente un trasporto di tipo intermodale;
- Multimodal Transport Operator (MTO): si interfaccia con il cliente, è colui che organizza il trasporto intermodale nella sua totalità;
- vettore stradale: si occupa del trasporto fisico su gomma;
- gestore del terminal: si occupa di trasbordare operativamente le ILU dai camion ai carri ferroviari e viceversa;
- trazionista: è il responsabile ferroviario del treno, esegue fisicamente la trazione, porta la merce da A a B secondo le indicazioni pianificate dal suo cliente (l'operatore commerciale del trasporto ferroviario) acquisendo le tracce orarie e le autorizzazioni dal gestore della rete;
- gestore della rete ferroviaria: è responsabile della circolazione dei treni, si occupa sia della manutenzione della rete fisica che della gestione del traffico

globale, è lui che determina i prezzi delle tracce e delle manovre di ingresso nel terminal;

- operatore commerciale del trasporto ferroviario: ha un ruolo centrale nel trasporto intermodale infatti si interfaccia con MTO, gestore del terminal e trazionista, si preoccupa di pianificare il trasporto ferroviario e si procura i carri ferroviari.

1.7 Conclusioni

Come descritto nel capitolo, il trasporto intermodale, in particolare strada-ferrovia, presenta svariati vantaggi in termini di sostenibilità ambientale (riduzione di inquinanti atmosferici), sociale (riduzione del traffico su strada), energetica (minor dispendio di energia) e di sicurezza (è utilizzato soprattutto per prodotti chimici pericolosi). Abbiamo sottolineato come potrebbe essere vantaggioso anche dal punto di vista economico in funzione della distanza da percorrere. Abbiamo inoltre evidenziato come i principali motivi del mancato sviluppo siano da ricercare nelle lacune gestionali, infrastrutturali, tecnologiche, di tracciabilità e trasparenza degli attori coinvolti nella pianificazione e gestione del tratto ferroviario; per superare queste lacune sarebbero necessarie direttive di incentivazione e regolamentazione a livello nazionale che in questo momento mancano.

2 Introduzione alla sicurezza

In questo capitolo ci occuperemo della sicurezza partendo dalla sua definizione generale, proseguendo con un excursus sull'evoluzione delle tematiche di sicurezza all'interno delle organizzazioni fino a contestualizzarla all'interno di una generica supply chain. Parleremo quindi di Supply Chain Security e della sua recente evoluzione, collocandola all'interno delle strategie di Risk Management e analizzando in termini generici gli impatti che le sue pratiche hanno sulle prestazioni di una supply chain. Infine ci ricollegheremo al trasporto intermodale andando ad analizzare le vulnerabilità che impattano sulla prestazione di sicurezza all'interno di una generica ILU supply chain.

Lo scopo di questa analisi è quello di delineare il nostro perimetro di indagine all'interno di un concetto poliedrico come quello della sicurezza e analizzarla in relazione alla supply chain, che in tale ambito si concretizza nelle pratiche di Supply Chain Security. Forniremo quindi un quadro generale sugli sforzi compiuti dalle organizzazioni in relazione alla prestazione di sicurezza.

Come vedremo, con il termine sicurezza sono compresi svariati concetti; noi ci occuperemo soltanto di un particolare aspetto di questa tralasciando la parte inerente alla sicurezza del personale sul luogo di lavoro, normato in Italia dal Testo Unico sulla Sicurezza sul Lavoro (TUSL).

Andremo poi a contestualizzare le tematiche di SCS all'interno del nostro ambito di riferimento, ossia il sistema di trasporto intermodale, che vede l'interazione di più attori che assieme compongono la "ILU supply chain", termine utilizzato nel progetto IMCOSEC (2010). Con il termine ILU supply chain intendiamo l'insieme di organizzazioni e attori che interagiscono tra di loro per portare dall'origine a destino il flusso di ILU (Intermodal Load Unit), ossia container, casse mobili e semirimorchi. In letteratura spesso gli autori fanno riferimento a container, ma le argomentazioni di nostro interesse non precludono la possibile estensione al concetto generico di ILU. Pertanto verranno considerati sinonimi i termini container, ILU, unità di carico e contenitore.

2.1 Premessa

La sicurezza, secondo la definizione ufficiale della lingua italiana, è definita come la *"condizione o qualità di chi e di ciò che è sicuro al fine di evitare comunque che si verifichi qualcosa di spiacevole, di dannoso o simile."* (Definizione da dizionario Zingarelli) [1]

In altri termini, la sicurezza , dal latino "sine cura", cioè "senza preoccupazione", può essere definita come la "*conoscenza che l'evoluzione di un sistema non produrrà stati indesiderati"*. (Wikipedia, 2011) [2]

La [1] evidenzia come la sicurezza possa essere riferita a persone (chi) o a luoghi, oggetti, informazioni (ciò), e quindi si focalizza su chi o cosa subisce "qualcosa di spiacevole, dannoso". La [2], invece, pone l'attenzione sul sistema in esame che, soggetto a minacce e pericoli nel tempo, può mutare e provocare danni (stati indesiderati).

A partire da una definizione così generica, è chiaro come il termine sicurezza si possa prestare a molteplici interpretazioni e ad essere considerato nelle sue svariate accezioni, a seconda dell'ambito e della disciplina che se ne occupa. Per ogni sistema in considerazione, le tematiche di sicurezza possono essere affrontate da un punto di vista normativo, manageriale, pratico, sociologico, organizzativo, tecnico, ingegneristico etc.

In particolare noi ci occuperemo di sicurezza secondo l'approccio manageriale, organizzativo, sociologico e in parte tecnico.

Considerata la generalità del termine sicurezza, è importante aver chiaro l'ambito di riferimento. Tuttavia, pur definendo l'ambito di analisi, non sempre è chiaro l'oggetto a cui la sicurezza può fare riferimento. Supponiamo, ad esempio, di parlare di sicurezza informatica: un'intrusione nel sistema informatico aziendale può essere finalizzata al reperimento di informazioni protette a danno di persone, oppure al danneggiamento delle informazioni stesse a danno del sistema informativo e dell'azienda. Quando si parla di sicurezza sul lavoro, sembrerebbe invece chiaro si riferisca alla sicurezza delle persone; tuttavia bisogna considerare anche che un incidente possa provocare danni diretti sulle persone e allo stesso tempo sull'azienda stessa, in modo diretto (danneggiamento impianti) o indiretto (mancata produzione, danneggiamento immagine). La sicurezza può essere infatti riferita a entità o persone, in accordo con la [1], nello stesso ambito di riferimento. La spiegazione risiede nel fatto che all'interno del termine italiano "sicurezza" collassano due distinti concetti che in altre lingue sono

espressi da parole differenti. Il termine inglese *security* corrisponde alla sicurezza del patrimonio tangibile e intangibile di un sistema, mentre il termine *safety* riguarda la sicurezza delle persone, intesa come loro incolumità.

A questo proposito precisiamo che la nostra analisi sulla sicurezza si è focalizzata su vari aspetti di un'organizzazione, ad eccezione delle questioni sulla sicurezza delle persone sul luogo di lavoro, normate dalla TUSL.

Oltre ad ambiguità, il termine italiano sicurezza è anche affetto da incompletezza: infatti, nella lingua italiana, il termine sicurezza non viene chiaramente differenziato da quello di prevenzione, perdendo quelli che sono gli aspetti legati alla protezione. Nella lingua inglese, il termine *security* è invece chiaramente definito come *"The prevention of and protection against assault, damage, fire, fraud, invasion of piracy, theft, unlawful, entry, and other such occurrences caused by deliberate action"* (www.businessdictionary.com).

Sicurezza non è solo prevenzione. In riferimento alla [2], la definizione sottolinea che un sistema deve essere in continua evoluzione per generare eventi indesiderati e quindi conoscere lo stato di sicurezza. Tuttavia, un sistema si può essere evoluto senza dar luogo a stati indesiderati, ma non per questo può essere ritenuto sicuro. La sicurezza totale si ha in assenza di pericoli, che, in senso assoluto, si tratta di un concetto difficilmente traducibile nella vita reale, per quanto possano essere efficaci le azioni preventive. Nel momento in cui si manifesta l'evento indesiderato, entrano in gioco le misure protettive.

Per poter fare valutazioni sensate della sicurezza, è necessario un approccio strutturato. Si può parlare di sicurezza quando la soglia di rischio percepita dalla società (ossia dalle persone coinvolte) è considerata accettabile. È quindi importante individuare un indice del rischio, se non possibile in termini quantitativi tramite il calcolo del prodotto tra probabilità di accadimento e magnitudo del danno, in termini qualitativi.

Questo spiega anche come mai al termine sicurezza devono fare riferimento entrambi i concetti di protezione e prevenzione, dal momento che la prevenzione agisce sulla riduzione della probabilità di accadimento, mentre la protezione sulla magnitudo del danno.

2.2 Evoluzione del concetto di sicurezza

Come evidenziano Williams et al. (2008), inizialmente le aziende hanno affrontato le tematiche di sicurezza da un punto di vista esclusivamente psicologico e sociologico a livello degli individui dell'organizzazione.

Le prime teorie sviluppate in ambito psicologico da Maslow nel suo celebre libro "Motivazione e personalità" (1954), richiamano il concetto di sicurezza intesa come "*bisogno primario all'interno di una gerarchia dei bisogni che spiega la sequenza di motivazioni che spingono l'individuo al lavoro"*. Un adulto medio, soddisfatti i bisogni fisiologici necessari per la sopravvivenza, deve poter contare su un ambiente di lavoro sicuro, stabile, ordinato, organizzato, conforme alle leggi e non soggetto a eventi imprevedibili e pericoli, tale da tutelare la sua incolumità. Le organizzazioni applicano politiche di sicurezza, che da questa prospettiva, diventano un mezzo per la soddisfazione del bisogno di stabilità e di protezione espresso dalle persone. Tali bisogni, secondo Maslow, sono fondamentali per stimolare la motivazione nei confronti del lavoro. Egli afferma che per raggiungere questo obiettivo, *"bisogna cercare di diminuire le ansie e le paure delle persone tramite una maggior consapevolezza".*

In ambito sociologico, altre teorie definiscono la sicurezza *"una percezione da parte delle persone di protezione contro i pericoli"* (Fairchild, 1944).

Recentemente, Kanti Bajpai (2003) ha ripreso il concetto di sicurezza dal punto di vista sociologico, proponendo una teoria sulla sicurezza in termini di "*Human Security"*. Richiamando in parte la teoria già citata di Maslow (1954), Bajpai afferma che la Human Security può determinare scelte personali, opportunità e propensione a guardare positivamente il futuro. *"La Human Security, studiata a livello di società, dovrebbe essere perseguita per poter effettivamente ottenere sviluppi globali. In particolare tale sicurezza viene raggiunta quando le persone raggiungono condizioni di vita e sostentamento entro uno standard.[…] Riassumendo, lo stato psico-sociale di benessere risulta essere la manifestazione della human security che abilita lo sviluppo futuro positivo della società".*

Quello che emerge dagli approcci alla sicurezza di carattere sociologico e psicologico, è un'evidente attenzione alla sicurezza intesa come *safety*, ossia incolumità e benessere delle persone. Tuttavia un contributo in chiave sociologica alla sicurezza, intesa non solo a livello di safety, è stato fornito dagli autori Fisher e Green (2004). Essi affermano che *"la sicurezza implica un ambiente stabile e prevedibile, in cui un individuo o un*

gruppo deve muoversi senza ostacolarlo o danneggiarlo e senza paura di tali disturbi e danni". A completamento della definizione di sicurezza, aggiungono che *"tale sicurezza può essere ottenuta dalle forze militari, dalle leggi, dal coinvolgimento di individui o organizzazioni, e dalle imprese. In particolare, si parla di sicurezza pubblica (Public Security) quando gli interventi sono finanziati dal Governo o dal settore pubblico, finalizzati alla sicurezza nazionale, mentre di sicurezza privata (Private Security) quando vengono ingaggiati individui, organizzazioni e altri servizi per la prevenzione da crimini, perdite o danni di individui, organizzazioni o strutture"* (Fisher e Green, 2004).

Il loro intervento ci permette di affrontar il tema sotto un approccio più pratico. Nell'analisi della letteratura è emerso che esiste una distinzione ricorrente tra sicurezza pubblica e privata, distinte in base alla tipologia degli sforzi di intervento e che nel corso degli anni il concetto di sicurezza ha subito un'evoluzione anche da questo punto di vista.

Un contributo recente alla definizione di Private Security è stato fornito da Strom, Berzofsky et al. (2010), i quali affermano che *"oggi, la Private Security è responsabile non solo della protezione di istituzioni nazionali e di infrastrutture, quali le industrie e gli stabilimenti produttivi, pubbliche utilities e il sistema di trasporto, ma anche della protezione del patrimonio conoscitivo e informativo delle aziende. Le aziende in questo campo, fanno sempre più affidamento a strumenti di sicurezza di varie tipologie (ad esempio protezione dei dipendenti e del patrimonio aziendale, investigazioni, screening dei potenziali entranti, sistemi di sicurezza dei sistemi IT, e molto altro ancora)"*.

Storm et. al nella loro ricerca raccolgono alcune considerazioni discordanti che si sono avute in passato sui confini di applicazione della private security, prima di dare una definizione più completa: Kakalik & Wildhorn (1971) hanno proposto una serie di strumenti finalizzati esclusivamente alla prevenzione e individuazione di azioni criminali; Bottom and Kostanosk (1983) hanno dichiarato invece che la private security fornisce protezione contro non solo i crimini, ma anche contro minacce come devastazioni, incidenti, errori umani, e pratiche anti-etiche.

Il tema della sicurezza nazionale, o di Public Security, è stato trattato dagli autori Newman and van Selm (2003), riprendendo il tema di Human Security di Bajpai: essi lo guardano dalla prospettiva governativa, il cui scopo sarebbe quello di proteggere le persone dai pericoli mortali dovuti a calamità naturali o attacchi terroristici.

Negli ultimi decenni si è verificato un crescente interesse verso la sicurezza privata, la quale si distingue sempre meno da quella pubblica. Molti sono gli autori che identificano l'assottigliarsi dei confini tra sicurezza pubblica e privata, in seguito all'attacco terroristico dell'11 Settembre 2001, a seguito del quale sono nate molte collaborazioni tra autorità pubbliche e settore privato per fornire un sistema paese più sicuro per cittadini, strutture e organizzazioni (Fisher e Green, 2004).
Oggi risulta quindi difficile fare una chiara distinzione tra interventi per la sicurezza pubblica e privata, come vedremo meglio in seguito parlando di Supply Chain Security e delle certificazioni nel paragrafo 3.1.

2.3 Supply Chain Security

La Supply Chain Security (SCS), principale oggetto di ricerca della nostra analisi bibliografica preliminare, è l'ambito di sicurezza entro cui si colloca il nostro focus. Dopo aver definito i concetti di Supply chain e di Supply Chain Security, andremo ad ripercorrere l'evoluzione e i trend in atto della SCS riscontrati in letteratura.

2.3.1 Definizioni

Secondo una definizione ufficiale, la supply chain è: *"The entire network of firms who interact to turn raw materials into finished goods and services and to deliver them to end customers"* (Supply Chain Council).
Più nel dettaglio, Closs e McGarrell definiscono la supply chain come *"la combinazione di organizzazioni e fornitori di servizi che gestiscono la fornitura di materie prime, la produzione, e la consegna di beni, dall'origine al consumatore finale. Le organizzazioni coinvolte direttamente nella supply chain sono fornitori di materie prime, produttori, grossisti, distributori e retailers. Altri stakeholders coinvolti nelle attività di una supply chain sono le autorità governative, trasportatori e terminal e operatori portuali*" (Closs e McGarrell, 2004).
Nonostante la Supply Chain Security sia un argomento ampiamente trattato, esistono pochissime sue definizioni formali.
Una definizione ufficiale definisce la SCS come *"il concetto entro cui vengono raggruppati i programmi, sistemi, procedure, tecnologie e soluzioni applicati per affrontare le minacce a cui sono soggette le supply chain e di conseguenza le minacce*

che mettono a rischio l'economia, il benessere fisico e sociale dei cittadini e delle organizzazioni" (Michel Donner, Cornelis Kruk, 2009).

Altre definizioni, di carattere informale, vanno a definire più in dettaglio le tipologie di minacce a cui sono soggette le supply chain. Secondo Closs e McGarrell (2004) *"SCS è l'applicazione di politiche, procedure e tecnologie con il fine di proteggere gli asset della supply chain (prodotti, strutture, attrezzature, informazioni e persone) da furti, danni o terrorismo e prevenire le intrusioni, il trasporto clandestino di persone e il contrabbando di armi per la distruzione di massa, nella supply chain"* (Closs e McGarrell, 2004) [3].

Burmeisters e Solovjovs (2009) affermano che *"il termine di Supply Chain Security (SCS) è riferito a un insieme di azioni volte a migliorare la sicurezza della supply chain. Esso combina le pratiche tradizionali di Supply Chain Management con i requisiti di sicurezza del sistema logistico e di trasporto, che è colpito da minacce quali attacchi terroristici, pirateria e furti"* [4].

Entrambe le definizioni sono concordanti e complementari, in quanto messe assieme illustrano in dettaglio gli elementi chiave di un approccio di SCS, ossia la tipologia di strumenti che utilizza e le minacce verso cui la supply chain si deve tutelare.

"Una supply chain sicura è una supply chain in cui sono state intraprese diverse misure per garantire un certo livello di sicurezza. Le misure di sicurezza possono essere prese in riferimento ai flussi fisici, informativi e/o monetari, o una combinazione di questi". (Veenstra 2005). Questa definizione mostra come la sicurezza di una supply chain sia un concetto molto ampio, che comprende sia una dimensione fisica e non fisica di sicurezza, sia misure preventive e correttive, come rappresentato in Figura 30.

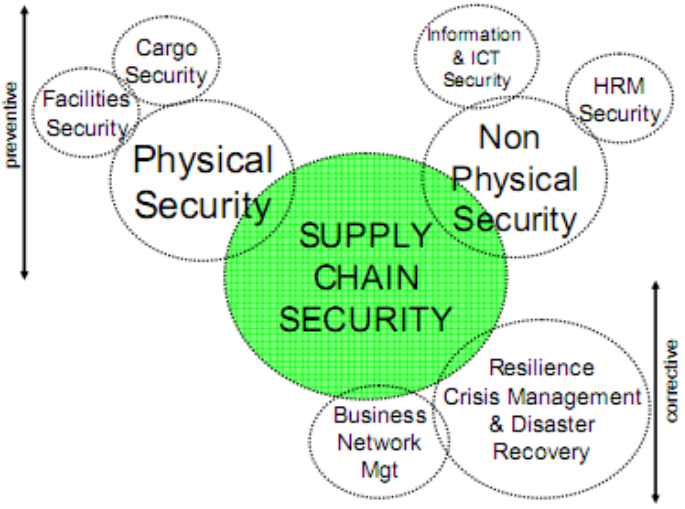


Figura 30: Componenti della Supply Chain Security (Van Oosterhout, et al. 2006)

2.3.2 Evoluzione della SCS

La Supply Chain Security è una tematica nata formalmente negli ultimi anni, ma trattata, seppur in modo non formale, già in passato. Hess e Wrobleski (1996) hanno evidenziato come *"attraverso la storia, le organizzazioni si sono trovate nelle condizioni di mettere al sicuro i beni durante il trasporto"*. L'esempio riportato è quello delle Ferrovie Americane che nel 1800, durante l'espansione verso ovest degli Stati Uniti, si trovarono ad affrontare furti di merci e saccheggi dei propri treni. Per tutelare carico e passeggeri, in quel caso furono applicate iniziative pubbliche (regolamentazioni e leggi) senza alcun successo, optando poi per un'incentivazione per i gestori della rete ferroviaria a ricercare in prima persona delle politiche da adottare per rendere il trasporto più sicuro. In questo caso viene individuato il primo chiaro esempio di SCS nella storia.

La [3] e la [4] sono definizioni piuttosto recenti (2009 e 2004), ma in realtà Williams et al. (2008) mettono in risalto come il focus della SCS sia cambiato nel corso degli anni, in particolare a partire dall'11 Settembre 2001.

Gli eventi dell'11 Settembre hanno fortemente influenzato la società e il business su scala globale. A seguito dell'attacco, il governo statunitense annunciò immediatamente un blocco aereo, e diverse leggi e regolamentazioni per proteggere il proprio Paese da ulteriori attacchi terroristici. Considerando il fatto che molte aziende americane operano su scala mondiale, tali decisioni hanno inevitabilmente interessato aziende e organizzazioni di tutto il mondo (IMCOSEC, 2010).

Secondo Williams et al. (2008), questa situazione ha messo in luce essenzialmente due criticità chiave: in primo luogo, *"è diventato evidente che, mentre le supply chain sono da un lato estremamente efficienti, dall'altro sono estremamente vulnerabili se colpite direttamente o indirettamente da eventuali "disruption"*- termine ricorrente nella letteratura non solo anglosassone sul tema, che fa riferimento a un *"evento imprevisto che genera un'interruzione delle normali attività, interruzione la cui durata e ampiezza dipende evidentemente dalla gravità dell'evento dirompente"* (Nassimbeni, 2009) - *dovute ad attacchi terroristici o catastrofi naturali*" (Williams et al., 2008); in secondo luogo, *"è emersa nelle supply chain la necessità di implementare anche degli strumenti anti terroristici a supporto della sicurezza"* (Williams et al., 2008).

La prima criticità fa riferimento ad alcune problematiche di Supply Chain Management, che come visto dalla definizione [4] possiede pratiche comuni alla SCS: infatti, *"le*

moderne supply chain sono esposte a rischi maggiori, e la principale causa è imputabile alla forte globalizzazione delle supply chain" (Williams et al., 2008). *"Le moderne reti interaziendali sono geograficamente più estese, coinvolgono un numero sempre crescente di attori eterogenei e di mercati in tutto il mondo, e veicolano una molteplicità di contenuti materiali e immateriali; questi fattori contribuiscono ad accrescere la complessità delle aziende e di conseguenza la loro vulnerabilità"* (Nassimbeni, 2009). Altri fattori che determinano una maggiore vulnerabilità, sono la diffusione delle logiche di gestione Just In Time (Donner e Kruk, 2009) e altri driver che elencheremo nel paragrafo 2.3.3.

A fronte di una crescente vulnerabilità, diventa crescente il bisogno di proteggere i clienti, la conoscenza, le infrastrutture, il brand, l'immagine e i dipendenti, e quindi aumenta il bisogno di attuare programmi di SCS, che diventano parte integrante e essenziale della strategia aziendale (Eggers, 2004; Sarathy, 2006). Questo spiega come mai in seguito all'11 settembre l'interesse verso le pratiche di SCS è aumentato da parte di tutti i membri della filiera.

In riferimento alla seconda criticità, è emerso che la visione attuale di SCS è cambiata significativamente dalla sua precedente concettualizzazione, proprio a partire dall'11 settembre. Prima, l'approccio di SCS si focalizzava essenzialmente *"on stopping product from leaving the supply chain"* (Thibault et al., 2006). Gli sforzi erano rivolti alla riduzione dei furti del carico, alla prevenzione dal trasporto clandestino e al contrabbando all'interno della SC. Oggi, invece, *"i supply chain manager possiedono la consapevolezza che bisogna affrontare i rischi a cui sono esposte le aziende, con un occhio puntato sul terrorismo. Gli eventi dell'11 settembre non hanno fatto altro che mettere in luce una minaccia pre-esistente, ma mai considerata reale"* (Burmeisters e Solovjovs, 2009).

Successivamente agli eventi dell'11 Settembre, l'approccio di Supply Chain Security ha subito ulteriori cambiamenti, riportati di seguito.

Da approccio funzionale a integrato

Tradizionalmente le tematiche di sicurezza sono state affrontate dagli attori coinvolti nelle attività delle supply chain, secondo un approccio funzionale. Ad esempio, *"mentre le aziende si focalizzavano sulla sicurezza dei propri asset, le autorità governative si focalizzavano esclusivamente sui ricavi, sulla riduzione di flussi illegali e sulla lotta anti-terroristica*" (Closs e McGarrell, 2004) Oggi, per realizzare un network sicuro, è

necessario integrare entrambi gli approcci e lavorare congiuntamente per garantire asset più sicuri, maggiori ricavi ed evitare il traffico illegale di armi, contrabbando e attacchi terroristici (Closs e McGarrell, 2004; Burmeisters e Solovjovs, 2009).

Da iniziative pubbliche o private, alla collaborazione dei due settori

È noto che il terrorismo ha la potenzialità di danneggiare non solo la SC ma anche le infrastrutture relative, l'ambiente che la circonda e le persone che vivono e lavorano in quel territorio. Perciò le organizzazioni private e le entità pubbliche, sono state spinte sempre di più dopo gli eventi dell'11 settembre a lavorare assieme per assicurare sia la pubblica sicurezza, sia un commercio di beni "sicuro". La sicurezza della supply chain oggi viene quindi considerato un obiettivo congiuntamente privato e pubblico (Gutierrez e Hintsa, 2006), come ben dimostrano i molteplici programmi di sicurezza intrapresi da differenti organizzazioni internazionali, agenzie governative e settori privati (IMCOSEC 2010), discussi nel paragrafo 3.1. Il ruolo del settore pubblico e le relazioni tra pubblico e privato sono una componente critica delle supply chain: infatti, *"se da un lato il settore pubblico deve valutare gli obiettivi di sicurezza e facilitare il trasporto –reso possibile solo tramite la cooperazione con il settore privato–, dall'altro i fornitori, produttori, trasportatori e altri attori della filiera devono riconoscere il merito alle autorità stesse di offrire una garanzia per il commercio internazionale. Questa interdipendenza spinge i due settori a collaborare tra di loro per rafforzare la sicurezza della supply chain"*(Closs e McGarrell, 2004).

Da programmi locali a programmi globali

Essendo la natura delle moderne supply chain "globale", è richiesto un approccio alla sicurezza che abbia un supporto a livello globale, da parte di organizzazioni non solo locali ma anche internazionali, necessario per garantire metriche, formazione e livello di innovazione comuni (Closs e McGarrell, 2004).

In seguito riportiamo alcune tendenze e sfide attualmente in corso per ottenere il massimo livello di sicurezza.

Da orientamento operativo a strategico

Chiaramente, gli eventi dell'11 settembre hanno avvicinato le aziende sempre di più alle pratiche di SCS. Le aziende stanno dedicando sempre più risorse e tempo a strategie di supply chain che permettono di gestire alcune questioni sulla sicurezza. Ma allo stesso tempo è necessario monitorare e mantenere le strategie, ai fini di non incorrere in

risultati disastrosi. Questo perché, come già anticipato, i programmi di SCS stanno iniziando ad essere percepiti dalle aziende come strategici, e non più di carattere operativo. *"Oggi la sicurezza è una parte centrale e essenziale, e tutti i partner della filiera devono sviluppare strategie e competenze sulla sicurezza"* (IMCOSEC 2010).

Da focus sulla singola azienda alla end-to-end supply chain

Un programma di SCS deve essere percepito come lo strumento per ridurre le vulnerabilità della supply chain, pertanto il suo principale obiettivo deve essere quello di ridisegnare una supply chain più robusta e resiliente in modo da evitare e mitigare gli impatti di una eventuale disruption. Per fare questo è necessaria la collaborazione non solo delle autorità governative - approccio integrato -, ma anche dei partner di tutta la supply chain. A tal proposito, Russell and Saldanha (2003) affermano che *"le aziende dovrebbero sviluppare una stretta partnership sia con le autorità governative, sia con i membri della supply chain, per affrontare le tematiche di sicurezza efficacemente"*. In quest'ottica, i costi di breve periodo per implementare misure di sicurezza possono essere bilanciati attraverso i benefici di lungo periodo che si otterrebbero dal miglioramento delle performance di sicurezza generali e da una migliore relazione con i clienti (Sarathy, 2005).

Considerando la forte interdipendenza tra i vari attori della filiera, è evidente che di fronte a una minaccia di grande rilievo, come può essere un attacco terroristico o una catastrofe naturale, vengono messe in pericolo le performance di tutta la filiera: *"tale ragione deve incentivare le aziende a ragionare in ottica di end-to-end supply chain e non pensare alle performance individuali"* (Closs e McGarrell, 2004; Burmeisters e Solovjovs, 2009). La difficoltà nell'adozione di una visione di questo tipo, risiede nell'intento di rompere i preconcetti, e perseguire un obiettivo comune, talvolta apparentemente a discapito delle performance individuali. In realtà basti pensare ai costi per implementare le misure di sicurezza necessarie, insignificanti se comparati alle potenziali perdite dovute a danni provocati all'intera infrastruttura delle supply chain e all'economia. Burmeisters e Solovjovs (2009) identificano i clienti come *"i pionieri di un approccio efficace di SCS integrato lungo la filiera per garantire la sicurezza a livello globale, tale da non ostacolare o rallentare il commercio globale, bensì facilitarlo"*. Essendo i clienti il punto finale della supply chain, *"le aziende sono in definitiva dipendenti dalla loro [clienti] soddisfazione e dovrebbero pertanto essere a*

loro volta interessate al raggiungimento di ottime performance di sicurezza della filiera globale" (Closs e McGarrell, 2004).

Da livello di 1st-tier supplier al 2nd, 3rd-tier supplier

Dal punto di vista operativo, *"le aziende non dovrebbero più focalizzarsi esclusivamente sulle procedure di sicurezza interna o al massimo dei 1st-tier suppliers, secondo la così detta prospettiva delle "quattro mura", bensì dovrebbero preoccuparsi anche della sicurezza delle procedure di tutti gli attori della filiera".* (Closs e McGarrell, 2004)

Da contingency plan a Crisis Management

Alla fine di tutto questo processo di cambiamento, risulta che le pratiche di una SCS non devono essere costituite solo da misure preventive ai furti e piani di emergenza per specifici stabilimenti produttivi o centri distributivi ("contingency plan"), ma supportate anche da un piano di "crisis management" che comprende componenti di planning, mitigation, detection, and response and recovery (Burmeisters e Solovjovs, 2009).

La Figura 31 riassume i requisiti attesi per un approccio di Supply Chain Security efficace, includendo sia i cambiamenti già consolidati, sia le tendenze e sfide in corso.

	Prima	→	Dopo
Misure	Prevenzione furti	→	Prevenzione furti e anti-terrorismo
Approccio	Funzionale	→	Integrato
Iniziativa	Pubblica o Privata	→	Pubblica e privata
Estensione	Nazionale/locale	→	Globale
Focus	Azienda	→	End-to-end supply chain
Visibilità	1st-tier suppliers	→	2nd, 3rd-tier suppliers
Supporto	Contingency Planning	→	Contingency planning & Crisis Mgmt
Impatto	Operativo	→	Strategico

Figura 31: Modello per il cambiamento dei requisiti della Supply Chain Security

2.3.3 Supply Chain Security e Risk Management

La SCS è stata collocata da alcuni autori all'interno delle pratiche di Risk Management della supply chain nel ruolo di componente strategica, diventando così fattore critico a

partire dall'11 settembre 2001. Più specificatamente, Williams et al. (2008) localizzano la pratica di SCS nel più ampio concetto di Supply Chain Risk Management.

Il *"Supply Chain Risk",* rischio di una supply chain, è *"un qualsiasi rischio che corrono il flusso di informazioni, materiali e prodotti tra il fornitore all'origine e il consumatore finale"*. (Jüttner et al., 2003)

La Supply Chain Risk Management (SCRM) è *"una disciplina del Risk Management che si propone di identificare e gestire il rischio all'interno di una supply chain, attraverso il coinvolgimento dei membri di una supply chain, con l'obiettivo di ridurre la vulnerabilità totale della supply chain"*. (Jüttner et al., 2003). Gli stessi autori propongono uno schema, illustrato in Figura 32, che identifica "*quattro componenti interdipendenti di SCRM:*

1. *risk sources;*
2. *risk drivers of supply chain strategy;*
3. *supply chain risk management strategies;*
4. *outcomes of supply chain risk".*

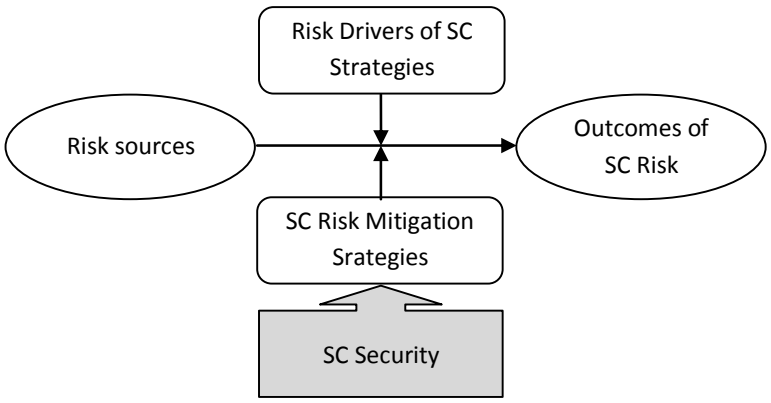


Figura 32: Framework di Supply Chain Risk Management (Jüttner et al., 2003)

Vediamo nel dettaglio ciascuna componente:

Risk sources

Jüttner (2005) suggerisce che le fonti di rischio rappresentano qualsiasi variabile che non può essere accuratamente predetta e che può condurre a una disruption della supply chain di qualsiasi tipo. Tra le fonti di rischio, l'autore identifica le seguenti tipologie di rischio:

- incidenti;
- catastrofi naturali;
- azioni socio-politiche (attacchi terroristici).

Risk drivers of supply chain strategy

Jüttner (2005) identifica cinque ragioni primarie che negli ultimi anni hanno portato le supply chain a modificare le proprie scelte strategiche, incrementando il rischio:

- globalizzazione;
- outsourcing;
- focus su l'efficienza, anziché sull'efficacia;
- specializzazione delle industrie;
- sistema distributivo centralizzato;
- supply base reduction.

Le cause che influenzano il rischio sono differenti a seconda del driver: i primi due driver rendono il network di aziende più complesso, in termini di numero delle relazioni da gestire e quindi più esposta a fonti di rischio, andando quindi ad aumentare la componente di rischio funzionale alla probabilità di accadimento di una disruption; i driver successivi agiscono sull'integrazione della supply chain, rendendola più integrata, quindi esposta a un minor numero di fonti di rischio ma con un impatto distruttivo superiore.

Supply chain risk management strategies

Le strategie di SCRM sono attività specifiche che le aziende intraprendono per ridurre il livello di rischio totale della supply chain. Queste strategie comprendono le generiche strategie di mitigazione del rischio (Jüttner et al., 2003), nelle quali si collocano i programmi di SCS come una specifica tipologia di strategia per ridurre il rischio globale (Closs et al., 2008). In particolare Williams et al. (2008) puntualizzano il fatto che la SCS si occupa della riduzione della probabilità di accadimento di disruption causate da azioni intenzionali, come il rischio di natura socio-politico. Per le altre tipologie di rischio non intenzionali il rischio permane, ma tramite SCS risulta comunque possibile ridurre il rischio globale delle supply chain.

Outcomes of supply chain risk

La principale conseguenza del rischio di una supply chain, è la vulnerabilità a disruption (Williams et al., 2008). Con vulnerabilità si intende *"l'esposizione a qualcosa che può disturbare la filiera"* (Christopher e Peck, 2004). *"L'incremento della vulnerabilità delle supply chain* - come abbiamo già discusso in precedenza - *è la conseguenza indiretta della globalizzazione e di altri fattori che le rendono maggiormente esposte alle minacce"* (Urciuoli 2009). Una maggiore esposizione alle minacce comporta un

incremento del livello di rischio rendendo le organizzazioni più suscettibili alle disruption, ossia più vulnerabili.

Secondo lo schema di SCRM di Jüttner (2003), risulta che la SCS è una specifica tipologia di strategia per la mitigazione del rischio. Williams et al. (2008), abbiamo visto come sostengano che i rischi siano principalmente causati da azioni intenzionali. La stessa scelta di focalizzarsi solo su fonti di rischio socio-politici, è stata effettuata recentemente del progetto IMCOSEC (2010). Questa tendenza deriva principalmente dal fatto che la maggior parte degli approcci di SCS sono nati proprio in seguito agli attacchi terroristici dell'11 settembre. IMCOSEC, prima di focalizzarsi su una specifica area della sicurezza, riconosce la presenza di più fonti di rischio possibili che possono compromettere la sicurezza di una supply chain, illustrate in
Figura 33.

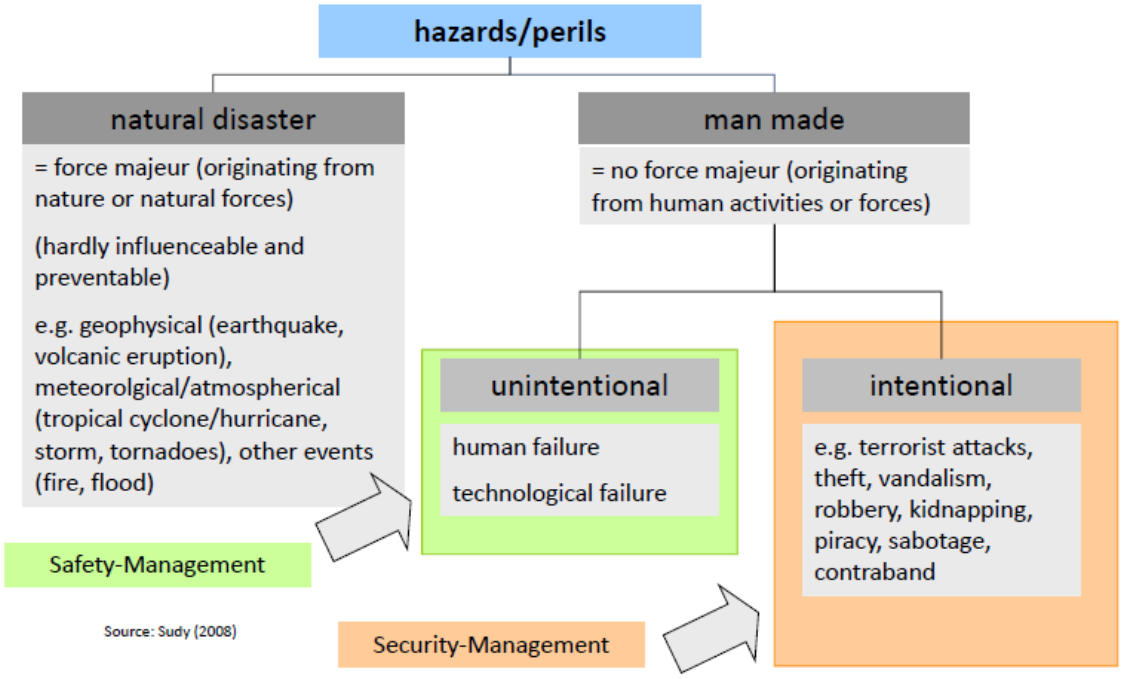


Figura 33: Minacce/pericoli di una supply chain (IMCOSEC, 2010)

Le minacce/pericoli[9] proposte da IMCOSEC si possono ricondurre alle stesse fonti di rischio di Jüttner (2005), raggruppando gli *"incidenti"* e i "*fattori socio-politici*" sotto un'unica categoria definita "man-made". In riferimento a quest'ultima categoria, IMCOSEC distingue incidenti e fattori socio politici in minacce "*non intenzionali*"*e*

[9] *"Con il termine minacce/pericoli (hazard/peril) si intende un pericolo potenziale non quantificato a cui la supply chain può essere esposta";* è diverso dal rischio, termine con cui si intende *"un evento a cui è possibile attribuire una percezione qualitativa o quantitativa del pericolo"* (Brignoli 2010).

"intenzionali": sulla prima agiscono le politiche di Safety Management mentre sulla seconda quelle di Security Management, che come spiegato sono l'effettivo oggetto del loro progetto.

Il fatto che le strategie di SCS vengano collocate all'interno del Risk Management, dimostra come sia importante conoscere i rischi e le minacce che una supply chain corre per sviluppare un efficace programma di SCS. L'analisi dei rischi è fondamentale per la sicurezza di qualsiasi organizzazione: conoscere il rischio vuol dire infatti avere una chiara percezione del livello di sicurezza della propria organizzazione.

Ogni fonte di rischio può essere classificata in base alla matrice di vulnerabilità, illustrata nella Figura 34, in funzione della loro probabilità di accadimento e della severità delle conseguenze (Sheffi e Rice, 2005).

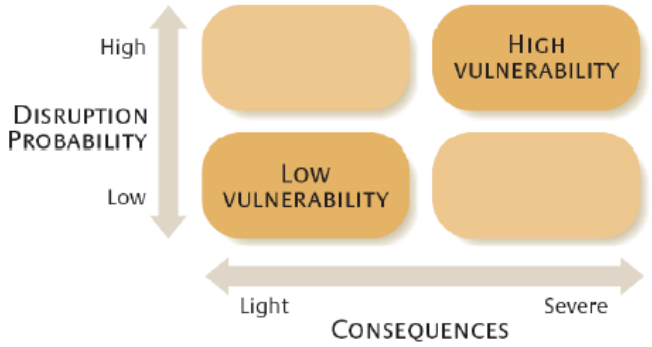


Figura 34: The Vulnerability Framework (Sheffi e Rice 2005)

Per ridurre la vulnerabilità, determinante della prestazione di sicurezza, si può quindi agire in due direzioni: ridurre la probabilità di accadimento di una disruption e/o ridurre l'impatto delle conseguenze di una disruption, ossia aumentare la resilienza.

Pertanto la SCS ha due differenti obiettivi: il primo è la riduzione della probabilità di accadimento degli eventi di rischio, che possono essere intenzionali o non intenzionali, (tralasciando quei rischi legati ai disastri naturali perché causati da forze maggiori); il secondo è la riduzione dei danni conseguenti ad essi (e anche da disastri naturali).

Secondo questa logica, la prestazione di sicurezza va a dettagliarsi in termini di "sicurezza preventiva" e di resilienza, come conferma Nassimbeni (2009): *"la vulnerabilità di una rete inter-aziendale alle disruption è il risultato di due caratteristiche tra loro correlate, ma che è opportuno distinguere: la sicurezza* - che per maggior chiarezza abbiamo chiamato "sicurezza preventiva" -, *"intesa come la capacità di un'impresa di monitorare e prevenire possibili fattori di destabilizzazione delle sue attività; la resilienza, intesa come la capacità di un'impresa che ha subito una*

disruption di ripristinare le normali attività. È dunque la capacità di reagire con rapidità a fronte di instabilità della rete, minimizzando i danni".

La prima rappresenta una misura statica del rischio e preventiva, la seconda una misura correttiva che cattura la capacità dinamica dell'impresa di recuperare rapidamente la condizione di regime (Nassimbeni, 2009).

La Figura 35 rappresenta la relazione che sussiste tra Supply Chain Risk Management e le prestazioni di sicurezza di una supply chain.

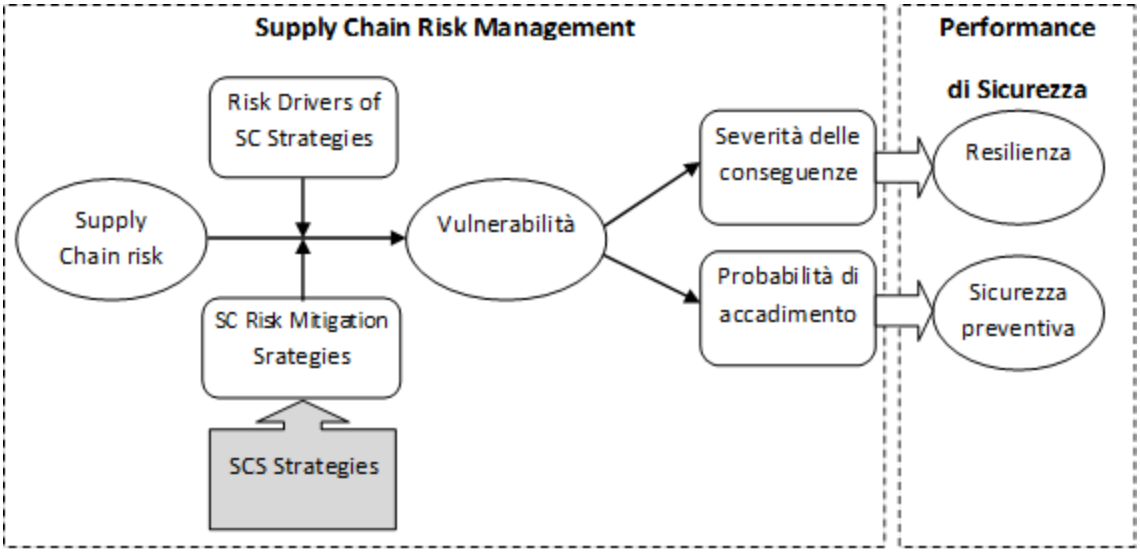


Figura 35: Supply chain risk management e performance di sicurezza

2.3.4 SCS e prestazioni organizzative di filiera

All'interno delle ricerche di SCS è molto diffusa la tematica inerente il legame che essa ha con le prestazioni organizzative. Tuttavia, fino ad oggi sono state condotte poche ricerche empiriche sulla relazione tra le attività di SCS e le performance. In seguito riportiamo alcuni esempi citati da Williams et al. (2008).

La società di consulenza Bearing Point ha dimostrato che esiste una relazione tra iniziative di SCS e benefici finanziari, prendendo in riferimento l'iniziativa dell'organismo Asia-Pacific Economic Cooperation, in cui vengono utilizzate le tecnologie RFID e i sigilli elettronici per tracciare i container dalla Thailandia ai centri distributivi in Seattle, WA. Con benefici finanziari si intendono un miglioramento della visibilità, nessun costo sull'import, riduzione delle scorte di sicurezza, miglior livello di servizio, maggiori profitti, e minori furti, il tutto stimato in un risparmio tra 150 e 2,000 dollari per container.

Allo stesso modo Eggers (2004) ha dimostrato che la partecipazione a iniziative di SCS di tipo governativo, come ad esempio il C-TPAT (paragrafo 3.1), hanno portato a un risparmio di costi di $378-462 per container per le aziende che importano beni in USA. Questi risparmi sono la risultante di un minor costo di transazione, maggior produttività del lavoro, minori furti, minori scorte, e minori overhead.

Infine, Peleg-Gillai et al. (2006), in collaborazione con IBM e The Manufacturing Institute, hanno studiato come le aziende industriali più innovative si approcciano alle iniziative per la sicurezza ottenendo importanti benefici, sconvolgendo il senso comune delle aziende nel vedere le iniziative di SCS solo dalla loro prospettiva negativa, ossia solo come una spesa che non porta ad alcun beneficio. Essi hanno infatti dimostrato che utilizzando un approccio proattivo alle iniziative di SCS alcune misure di sicurezza possono portare a delle performance organizzative positive, impattando su alcune aree prestazionali da loro identificate nella gestione delle scorte e livello di servizio, visibilità, efficienza, resilienza e cutomer relationship. In definitiva, tramite lo studio di un campione di aziende, hanno osservato benefici positivi sulle attività interne e in termini di relazioni con i partner e i clienti e di profittabilità, da parte degli sforzi in direzione della SCS, affermando che *"better security drives business value".*

In linea con questi risultati, altre ricerche, seppur in termini concettuali, evidenziano in che modo gli sforzi per la sicurezza di una supply chain abbassano i costi totali, aumentano la visibilità, la customer satisfaction e la profittabilità (Rice e Spayd, 2005; Sarathy, 2006; Daschkovska et al., 2008), proteggono il brand e preservano le quote di mercato. (Eggers, 2004).

Il tema più trattato in letteratura è sicuramente il rapporto tra le prestazioni di sicurezza (resilienza e sicurezza preventiva), efficienza, visibilità e efficacia.

In seguito dettaglieremo ciascuna relazione.

Sicurezza e visibilità

La visibilità è uno dei temi più ricorrenti tra le misure di SCS e i requisiti per la mitigazione del "rischio di sicurezza".

Lee e Wolfe (2003) sostengono che *"i rischi della supply chain possono essere ridotti o eliminati incrementando la visibilità, intesa come trasparenza in riferimento allo stato del flusso fisico, delle informazioni e del denaro. La trasparenza di una supply chain incrementa quando vengono rese disponibili le informazioni in maniera tempestiva e con alta qualità nell'intera catena".* Tali informazioni sono essenzialmente di tre

tipologie: del carico, del processo (tracking e tracing) e sull'integrità dei beni e dei trasportatori. (van Oosterhout et al., 2006)

Visibilità ed efficienza

Sarathy (2006) afferma che gli investimenti in SCS *"possono avere degli impatti positivi sulla riduzione totale dei costi della supply chain attraverso una maggiore visibilità in-transit dei tempi e flussi e delle informazioni relative allo status del trasporto. Migliori, accurate e tempestive informazioni della supply chain permettono di gestire la supply chain con minori scorte[…] gli operatori della supply chain possono individuare dove si manifesta un ritardo in modo che la supply chain venga migliorata e diventi più efficiente"*

Rice e Spayd (2005) affermano che *"la visibilità nella supply chain è un prerequisito per incrementare la sicurezza, ma è anche la base per altri benefici collaterali come l'incremento dell'efficienza logistica. […] La visibilità è importante perché la sicurezza della supply chain perché può generare informazioni che aiutano nella mitigazione delle vulnerabilità"*.

Sheffi (2005) osserva invece come *"la visibilità nella catena può aiutare a indentificare in anticipo le fonti di rischio (prevenzione). Può anche aiutare nell'anticipata identificazione delle disruption (detenzione) e rivelare gli impatti delle debolezze strutturali, e quindi delle vulnerabilità"*.

Sicurezza ed efficacia

Alcune misure di sicurezza sono in grado di migliorare l'intero processo logistico e quindi il livello di servizio, che si traduce in un ulteriore miglioramento delle performance organizzative (Gutierrez e Hintsa 2006). Peck (2005), analizzando le performance che si possono ottenere in termine del flusso di beni e processi, riconosce un aumento del livello di servizio attraverso un impatto significativo sulla riduzione di danni, perdite e ritardi.

Performance a livello di customer satisfaction, inventory management, livello di servizio e affidabilità trattate dai vari autori (Williams et al. 2008, Peleg-Gillai et al. 2006, Eggers 2008) sono tutte ricondotte alla prestazione di efficacia.

Sicurezza ed efficienza

Come si può osservare dalla Tabella 8 sulle densità degli autori riportata a fine capitolo, molti studi si sono focalizzati su come ottenere benefici in termini di sicurezza e di efficienza simultaneamente. Questo perché, come già anticipato, spesso le aziende

hanno una percezione negativa delle iniziative di sicurezza e lo vedono come un costo puro e l'intento delle ricerche è proprio quello di dimostrare il contratìrio. Le ricerche che affrontano la SCS dal punto di vista delle prestazioni, evidenziano quasi sempre l'esistenza di un legame positivo tra prestazioni di sicurezza (sicurezza preventiva e resilienza) ed efficienza (e conseguentemente alla profittabilità), che come abbiamo visto è il legame che si presta meglio ad essere dimostrato quantitativamente.

Hess and Wrobleski (1996), collegano la maggior efficienza delle operation interne aziendali alle seguenti motivazioni: riduzione di costi operativi (costi per la rilevazione di crimini; costi di investigazione e prosecuzione di sospetti, misurati in termini di perdita di tempo del personale addetto alla sicurezza e ai manager); riduzione di costi opportunità (alti costi di assicurazione, riduzione dei profitti, perdita di produttività, danneggiamento della reputazione, peggior livello di servizio, minacce alla sopravvivenza del business). Per quanto riguarda i costi operativi, *"possono manifestarsi benefici derivanti anche da altri fattori secondari (qualità dei prodotti, la funzione di marketing..) per i quali risulta più difficile la stima imputabile solo alle iniziative di sicurezza"* (Gutierrez e Hintsa, 2006).

Una maggiore efficienza è raggiungibile anche grazie ad approcci inter-organizzativi di SCS, tramite l'allineamento dei piani e degli obiettivi lungo tutta la filiera come avviene per le normali strategie moderne di SCM (Burmeisters e Solovjovs, 2009). L'idea di Burmeisters e Solovjovs (2009), Lee e Whang (2005) e altri autori è quella di applicare delle strategie per la mitigazione del rischio utilizzando la filosofia di base dei programmi per il miglioramento della qualità, come il TQM. "*Questi programmi permettono di pensare alla sicurezza della supply chain in termini di prevenzione, controllo dei processi, e di disegnare dei miglioramenti che aumentano l'affidabilità della filiera e allo stesso tempo la riduzione dei costi e aumento di produttività. L'assunto di base di questa prospettiva è che i difetti possono essere veramente costosi per tutta la supply chain*" (Burmeisters e Solovjovs, 2009).

Tuttavia, la letteratura è ricca anche di discussioni critiche sul rapporto tra sicurezza e efficienza. Willis e Ortiz (2004), nella loro ricerca sul sistema del network di trasporto di container, individuano alcune *"capabilities of supply chain performance"* interconnesse tra di loro da considerare nell'implementazione di misure di sicurezza. Tali misure sono:

- efficienza*: "capacità core del sistema nel garantire un flusso che sia veloce, economico e consistente";*

- affidabilità del trasporto: "*capacità del sistema di assicurare l'arrivo della merce entro specifiche finestre di consegna subendo il minor numero di perdite, furti e incidenti";*
- trasparenza del trasporto: "*capacità di sapere cosa si sta muovendo nel sistema, a garanzia che il carico sia autorizzato e trasportato legalmente";*
- tolleranza agli errori: "*capacità del sistema nel rispondere alle disruptions e errori di componenti isolati senza comportare l'arresto dell'intero sistema";*
- resilienza: "*capacità di un'impresa che ha subito una disruption di ripristinare le normali attività nel minor tempo possibile".*

A valle della loro analisi, emergono principalmente due considerazioni in merito alle relazioni che gli strumenti di sicurezza hanno con l'efficienza.

In primo luogo, *"le prestazioni di efficienza e di sicurezza di una supply chain, sono distinte ma interconnesse tra di loro: questo significa che quando si valutano le misure di sicurezza bisogna considerare tutti gli aspetti delle prestazioni di una supply chain. Ad esempio, il furto è un rischio per tutti gli attori della supply chain; tuttavia, gli sforzi per migliorare questo aspetto della sicurezza potrebbero impattare in modo positivo o negativo sull'efficienza della supply chain"* (Willis e Ortiz 2004).

Migliorare le prestazioni di resilienza e di tolleranza agli errori non sempre migliora l'efficienza; anzi, *"se si lavora sotto le "condizioni operative normali" si potrebbero avere effetti addirittura negativi"* (Willis e Ortiz 2004). La spiegazione risiede nel fatto che entrambe le *capabilities,* comportano il coinvolgimento di risorse aggiuntive – tali da garantire ridondanza e flessibilità, determinanti di una supply chain resiliente (Caniato e Rice, 2003) - che sotto condizioni operative normali, vengono intese come un "cattiva allocazione" delle risorse. *"Per evitare percezioni negative delle misure di resilienza, è importante considerare il sistema sia in condizioni operative "normali", sia di "emergenza". Le prestazioni sono per natura interconnesse tra loro e questo dimostra come mai gli attori della supply chain tendono sempre a evitare o a compensare i requisiti di sicurezza per non danneggiare le prestazioni di efficienza"* (Willis e Ortiz, 2004).

In secondo luogo, le iniziative per migliorare la sicurezza sono focalizzate sulla prevenzione al contrabbando e agli attacchi terroristici, con un minor focus invece sul miglioramento delle prestazioni di resilienza, come abbiamo già potuto riscontrare dalle considerazioni di altri autori.

Altri autori (Sheffi, 2001; Nassimbeni, 2009) hanno evidenziato in letteratura il trade-off esistente tra le prestazioni di sicurezza e di efficienza. Alcune strategie di SCS possono portare a un peggioramento in termini di efficienza, ma d'altra parte anche strategie pensate in ottica di supply chain efficiente possono portare a un peggioramento delle prestazioni di sicurezza. Nassimbeni (2009) nella rielaborazione del contributo di Sheffi (2003), propone una rassegna di fattori che mettono in contrasto le prestazioni di sicurezza e di efficienza, illustrati in Tabella 7.

Tabella 7: Scelte che generano trade-off tra le prestazioni di sicurezza e efficienza

Fattori	Trade-off	Motivazione
Ripetitività vs. imprevedibilità	Efficienza vs. sicurezza	*"L'accumulazione di esperienza sui percorsi tradizionali favorisce le economie dinamiche, con un guadagno di efficienza. Tuttavia privilegiare il "noto"ed il "consolidato" da una parte ostacola l'individuazione di opportunità migliori, dall'altra allenta la vigilanza sui potenziali imprevisti. Non solo: deliberati fattori di perturbazione quali il furto, la contaminazione o la manipolazione volontarie vengono favoriti dalla ripetitività dei processi. Da questo punto di vista, variazioni rispetto alla routine, ad esempio il cambio di password o la rotta dei trasporti, ostacolano possibili disruption."*
Fornitore o distributore singolo vs. multiplo ed estero vs. domestico	Efficienza vs. sicurezza	*"La frammentazione dell'ordine aumenta il costo complessivo della transazione, dal momento che alcuni costi si moltiplicano: costi di trasporto, di programmazione e controllo, di set-up dei materiali, di amministrazione. Nel contempo può essere necessario moltiplicare attrezzature specifiche, ad esempio gli stampi. In definitiva, la frammentazione dell'ordine impedisce vantaggi di scala. Tuttavia il single-sourcing denuncia tutte le vulnerabilità che derivano dall'esistenza di un unico canale di ingresso o di uscita. Considerazioni per certi versi simili riguardano la selezione di fornitori prioritariamente sulla base del prezzo/ costo piuttosto che sulla base anche di fattori non-price. La ricerca ostinata del vantaggio di costo può privilegiare interlocutori meno affidabili, o la cui localizzazione off-shore introduce una molteplicità di elementi di rischio."*
Centralizzazione vs. Decentramento	Efficienza vs. sicurezza e resilienza	*"La concentrazione spaziale delle risorse facilita il loro controllo e coordinamento e riduce la superficie di esposizione delle connessioni. Una disruption che agisce localmente può tuttavia ledere contemporaneamente più risorse. Viceversa, un'organizzazione distribuita è più difficilmente paralizzabile da disruption che intervengono a livello locale, inoltre può meglio giocare sulla sostituzione*

		di risorse o percorsi, a scapito tuttavia di una maggiore vulnerabilità delle connessioni."
Collaborazione vs. segretezza	Efficienza vs. sicurezza	*"La collaborazione operativa e la condivisione di informazioni sono necessarie per la realizzazione di filiere integrate, con vantaggi di reattività ed efficienza del flusso. Ma la condivisione di dati, conoscenze tecnologiche e modalità operative incrementa il rischio di intercettazione di informazioni riservate, di distorsione di informazioni, di comportamento opportunistico di soggetti interni o esterni alla filiera. La condivisione amplia in definitiva il perimetro entro il quale distribuire gli strumenti di prevenzione e recupero, con una minore efficacia degli stessi."*
"Leaness" vs. ridondanza di risorse	Efficienza vs. sicurezza	*"Le risorse in eccesso (impianti o macchinari produttivi, risorse umane o scorte), sono elementi "grassi" delle organizzazioni, ma che nei momenti di crisi tornano utili. Si tratta evidentemente di valutare se il costo del loro mantenimento in condizioni di normalità giustifica il loro valore in condizioni diverse."*

Nassimbeni (2009), in risposta al trade-off tra le prestazioni, suggerisce che è necessario *"definire un valore di accettabilità del rischio, un valore cioè compatibile con i costi necessari per prevenirlo e intervenire sulle possibili emergenze".*

Mappa delle relazioni

Riassumendo tutti i legami tra le prestazioni riscontrati in letteratura, è possibile rappresentare una mappa delle relazioni attraverso lo schema in Figura 36.

Tale schema riprende la relazione tra strategie di SCS e la prestazione di sicurezza rappresentata in Figura 35, ampliandola con gli impatti che hanno anche su altre prestazioni. Si nota come le pratiche di SCS abbiano effetti diretti (e indiretti tramite una miglior trasparenza) sulla sicurezza e efficienza, indiretti sull'efficacia e generino un trade-off tra le prestazioni di sicurezza e di efficienza.

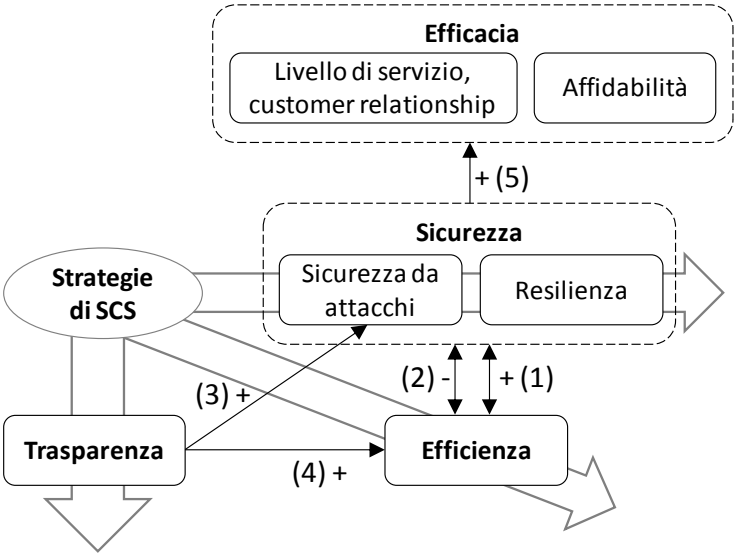


Figura 36: Mappa delle relazioni tra prestazioni organizzative

Nella Tabella 8 sono stati inseriti gli autori, in parte già citati, che hanno analizzato i legami tra le prestazioni.

Tabella 8: Letteratura sulle relazioni tra prestazioni organizzative

Relazione	Prestazioni	Autori
(1)	Sicurezza → + Efficienza Efficienza → + Sicurezza	Hess e Wrobleski (1996), Closs e McGarrell (2004), Eggers (2004), Gonzalez (2004), Lee e Whang (2005), Rice e Spayd (2005), Sarathy (2006), Peleg-Gillai et al. (2006), Gutierrez e Hintsa (2006), Burmeisters e Solovjovs (2009), Donner e Kruk (2009)
(2)	Sicurezza → - Efficienza Efficienza → - Sicurezza	Sheffi (2003), Willis e Ortiz (2004), Sarathy (2006), Nassimbeni (2009)
(3)	Visibilità → + Sicurezza	Lee e Wolfe (2003), Eggers (2004), Sarathy (2006), Van Oosterhout et al. (2006), Gutierrez e Hintsa (2006)
(4)	Visibilità → + Efficienza	Rice e Spayd (2005), Sheffi (2005), Sarathy (2006)
(5)	Sicurezza → + Efficacia	Rice e Spayd (2005), Gutierrez e Hintsa (2006), Sarathy (2006), Peleg-Gillai et al. (2006)

2.4 Sicurezza nell'ILU Supply Chain

Esistono molteplici ragioni per cui le pratiche di SCS si sono focalizzate prevalentemente sul sistema che gestisce il flusso di ILU all'interno delle supply chain. Come abbiamo già discusso, il fenomeno della globalizzazione ha avuto delle forti

ripercussioni sulla supply chain e sugli sforzi di Supply Chain Security. In particolare le maggiori ripercussioni si sono manifestate a livello del sistema distributivo, come emerge dalle considerazioni di Sarathy (2005): *"la globalizzazione è il tema centrale dell'economia globale, in quanto coinvolge un numero sempre crescente di risorse, produttori, industrie localizzate in tutto il mondo. L'infrastruttura fisica, fondamentale per servire i mercati internazionali conseguenti alla globalizzazione, è sotto minaccia; questo compromette le capacità delle aziende di tutto il mondo di commerciare beni e servizi internazionalmente"*.

Con l'aumento del livello di globalizzazione delle supply chain, in questi ultimi anni si è verificato un crescente aumento di volumi di trasporto multimodale.

Alcuni dati forniti da una ricerca condotta da Downey (2006), mostrano che il commercio globale è cresciuto con un tasso annuale del 10% in questi ultimi anni, con un aumento del tasso annuale del 7% dei flussi via container. Dati recenti forniti da Kim et al. (2009) riportano che il 90% del commercio è effettuato su scala globale, con la prevalenza di carichi trasportati via container. Più precisamente, secondo una stima di Ihs Fairplay, società tedesca di studi statistici, il traffico di container nel 2010 si è attestato intorno ai 115 milioni di TEU (container da 20 piedi) a livello globale, con una crescita dell'11,7% rispetto ai 103 milioni movimentati nel 2009 e con una previsione di incremento medio annuo nei prossimi cinque anni, del 6,3% (Il Sole 24 Ore 2009).

Prendendo in considerazione questi dati, è possibile capire l'importanza che il ruolo dei container detiene nelle supply chain.

Sarathy (2005) illustra alcuni risultati di una ricerca empirica, condotta dalla società A.T. Kearney nel 2004, significativi per le tematiche di sicurezza: chiedendo ai supply chain manager la loro percezione sulle sfide che una supply chain deve intraprendere, essi hanno individuato *"assure container security"* tra le più importanti, oltre a considerazioni manageriali sulla riduzione delle scorte, della variabilità dei lead time e degli stock-out. Successivamente, la stessa ricerca propone una serie indicazioni su cosa deve fare un'organizzazione per garantire la sicurezza del trasporto di container.

Per capire come migliorare la sicurezza di una supply chain e quindi ridurne la vulnerabilità, è importante comprendere quali sono i punti soggetti a rischio in tutta la filiera. *"Le disruption di una supply chain possono verificarsi in diversi punti lungo tutta la filiera"* (Sarathy, 2005). Inoltre, come abbiamo visto precedentemente parlando di globalizzazione, Sarathy identifica nella *"infrastruttura fisica fondamentale per*

servire i mercati internazionali conseguenti alla globalizzazione", in altre parole la ILU supply chain la parte oggi più critica e soggetta a minacce.

"I container sono uno delle maggiori fonti di preoccupazione della SC, dal momento che i container sono stati usati per il contrabbando di clandestini, armi e droghe" (Sarathy, 2005). In completo accordo sono Crist et al. (2005), i quali affermano che *"non c'è stato un solo caso isolato di incidente in cui i terroristi hanno cercato di usare un container come mezzo di trasporto per armi a distruzione di massa o per altri scopi"* Un caso di rilievo si è verificato proprio in Italia, nel porto di Gioia Tauro, nell'ottobre del 2001, con la cattura di un presunto terrorista nascosto in un container trasportato su una nave diretta verso il porto di Halifax. Il container era equipaggiato con un letto, un bagno e conteneva certificati falsi, mappe di aeroporti e security pass.

Inoltre, l'esplosione, o solo il ritrovamento di armi di distruzioni di massa (WMD, weapon of mass destruction) in un container, può portare a conseguenze disastrose. O'Hanlon, Gerencser et al. (2002) stimano che l'esplosione di WMD e la conseguente chiusura di un porto possono costare mille miliardi di dollari, mentre solo la chiusura del porto, per disinnescare un WDM, potrebbe costare circa 58 miliardi di dollari.

Closs e McGarrel (2004) riportano un altro esempio storico che ha spinto a rafforzare la sicurezza delle ILU supply chain. È il caso del furto in Messico nel Maggio 2003 di un intero autocarro che trasportava 8 tonnellate di cianuro, recuperato dopo due settimane di ricerche da parte delle forze dell'ordine. Questo incidente ha messo in luce le minacce potenziali che incorrono nel trasporto di merci pericolose, e i possibili vantaggi che possono derivare dall'utilizzo di procedure di sicurezza e tecnologie per il tracking del carico. In realtà i container rappresentano solo una parte delle problematiche di sicurezza. "*Anche gli operatori della ILU supply chain hanno bisogno di essere sicuri. La sicurezza deve infatti riguardare ogni elemento, attore e persona all'interno della supply chain; questo significa inglobare nelle verifiche di sicurezza di una ILU supply chain tutti i partner, fornitori di beni e di servizi*" (Sarathy, 2005). Le aziende partner e le autorità governative devono collaborare per monitorare e salvaguardare la sicurezza in tutti i punti attraversati dalle ILU, sia che queste si trovino in mezzo al mare, in aria, su strada o su ferrovia.

2.4.1 La vulnerabilità dell'ILU supply chain

Peck (2005), in uno dei primi studi sulla vulnerabilità di una supply chain, ha proposto un framework che identifica le vulnerabilità in base a quattro livelli differenti e

interconnessi di una supply chain, come mostrato in Figura 37: Framework a livelli di analisi della vulnerabilità (Peck 2005):

- Livello 1: flusso di valore, di prodotto, di informazioni e di processo
- Livello 2: risorse e infrastrutture (fisse o mobili)
- Livello 3: network organizzativi e inter-organizzativi (relazioni contrattuali e commerciali)
- Livello 4: ambiente (sociale e naturale)

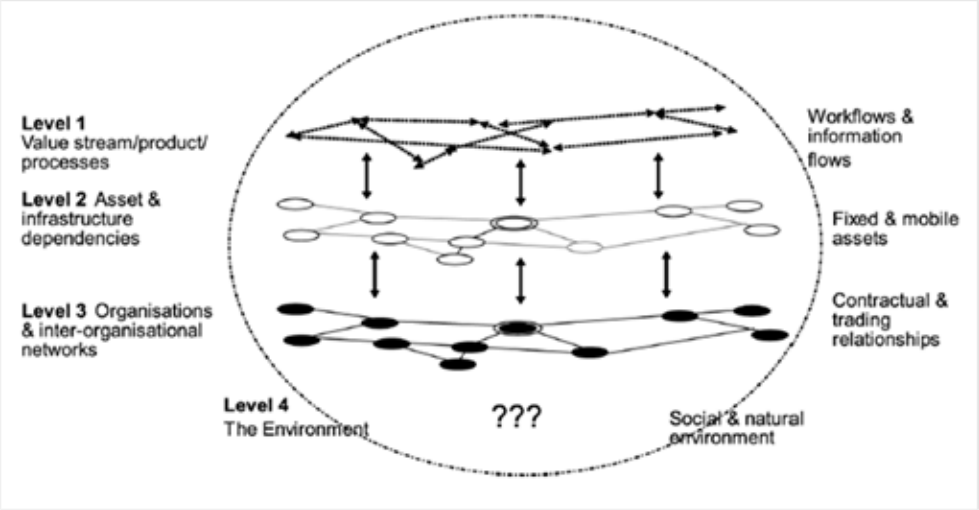


Figura 37: Framework a livelli di analisi della vulnerabilità (Peck 2005)

Al livello 1 le vulnerabilità vengono ricondotte al sistema logistico di una supply chain, che deve essere snello e agile ma per questo motivo risulta esposto a numerosi rischi. Al livello 2 la supply chain viene considerata come il convogliatore di beni e informazioni, pertanto le vulnerabilità sono determinate da minacce che possono interessare siti produttivi, centri distributivi, strutture logistiche, informazioni, altre strutture comunicative e l'intero network di trasporto che collega il fornitore al cliente finale. Al livello 3 la supply chain è vista dal punto di vista delle strategie e della prospettiva manageriale, in cui la gestione organizzativa, la collaborazione e la competizione diventa un importante fattore per la valutazione della vulnerabilità. Infine al livello 4 la supply chain viene collocata in un'ampia prospettiva macroeconomica, in cui vengono considerati i fattori politici, economici, sociali, legislativi e tecnologici.

Secondo Peck (2005) questo framework è uno strumento eccellente per spiegare la natura e la dinamicità dei rischi di una supply chain. L'interconnessione tra i vari livelli

implica che le azioni per ridurre i rischi in un punto della supply chain modifichino il profilo di vulnerabilità di tutti i livelli.

In alcune sue ricerche, Sarathy (2005, 2006) identifica sei elementi di una supply chian in cui è opportuno analizzare le vulnerabilità che si possono ricondurre al Livello 1 e 2 del framework di Peck. Sarathy, infatti, coerentemente al framework multi-livello, considera la supply chain come un insieme di elementi che muovono beni sotto forma di ILU e informazioni ad esse relative. Tali elementi sono i seguenti:

- stabilimenti produttivi, in cui vengono realizzate o assemblate le componenti;
- unità di carico, il cui trasporto è l'obiettivo principale della supply chain;
- fornitori, partner e organizzatori del trasporto nella supply chain, quali spedizionieri e compagnie di trasporto via strada, ferrovia, mare o aereo;
- strutture logistiche della supply chain, quali i magazzini in cui avviene il consolidamento del carico e i terminal entro cui le ILU sono trasbordate;
- persone che hanno accesso ai container e alle strutture della supply chain, come i dipendenti, trasportatori e intermediari;
- informazioni, in particolare il manifesto del carico, informazioni confidenziali e dati.

Questo schema dimostra quanto il problema non sia legato esclusivamente alla sicurezza fisica del container, ma riguarda anche le strutture e gli attori che gestiscono, manipolano e trasportano tale contenitore.

In seguito tratteremo ciascun elemento, evidenziando le principali minacce che possono compromettere la sicurezza di una supply chain.

Stabilimenti produttivi

Sarathy (2005) riconduce le problematiche di sicurezza che interessano gli stabilimenti produttivi prevalentemente a furti o manipolazioni o sostituzioni del carco originale, con prodotti che possono mettere in pericolo le persone e causare conseguenze dannose all'organizzazione (come perdite monetarie o di reputazione dell'azienda). Le minacce a questo livello possono provenire anche dagli stabilimenti dei partner e dei sub-contractor.

Unità di carico

Una volta reso sicuro il luogo di produzione o assemblaggio, il focus si muove verso il container che trasporta i prodotti. Le problematiche di sicurezza, a questo punto includono: *"il monitoraggio e il caricamento delle merci nel container, l'integrità del*

container, il monitoraggio di tentativi di manipolazione del contenuto del container durante il viaggio e la verifica dell'integrità dei container al loro arrivo" (Sarathy 2005). Daschkovska (2010) pone in evidenza che un container può subire intrusioni prima di essere chiuso e sigillato, ma anche successivamente durante il viaggio. Crist et al. (2005) sottolineano che ogni tipologia di ILU può apportare rischi differenti alla supply chain. Essi affermano che esistono *"il significativo numero di ILU specializzate sono rilevanti da una prospettiva di sicurezza, in quanto ciascuna tipologia rappresenta un particolare rischio: i tank container pieni non sono facilmente scannerizzabili, il loro contenuto è difficile da visionare e potrebbero contenere sostanze pericolose; i container refrigerati hanno muri isolati e apparecchiature per la refrigerazione, entrambe delle quali potrebbero essere usate per nascondervi ordigni; infine i container scoperti sono vulnerabili agli accessi non autorizzati attraverso il telone che li ricoprono, anche se in realtà sono i contenitori più facilmente ispezionabili"*. Oltretutto anche i container vuoti possono rappresentare un rischio (Daschkovska, 2010 e van Oosterhout et al., 2006). A tal proposito van Oosterhout et al., affermano che esistono pochi strumenti e controlli di sicurezza per la gestione dei vuoti (sia nei depositi che durante il trasporto verso il luogo di carico). Gli strumenti che agiscono sulla sicurezza del carico vengono ricondotti alla categoria di *"Cargo Management"*(paragrafo 3.2.2)

Fornitori, partner e organizzatori del trasporto

Le aziende di trasporto e gli spedizionieri internazionali sono elementi chiave della supply chain, in quanto *"il container passa attraverso le loro mani e possono rappresentare una minaccia se le procedure adottate non sono adeguate"* (Sarathy, 2005), oppure possono essere loro stessi i fautori di furti e manipolazioni (Daschkovska, 2010). Per questo motivo Sarathy (2005) suggerisce che queste figure devono essere motivate, dai propri clienti, ad utilizzare le pratiche di sicurezza conformi a programmi volontari internazionali per la sicurezza. Gli strumenti che agiscono sulla sicurezza delle organizzazioni coinvolte nel trasporto intermodale sono collocati all'interno della categoria di *"Business Network e Company Management System"* (paragrafo 3.2.6).

Strutture logistiche

In questi punti della supply chain *"il container può essere soggetto a manipolazioni o furti da parte di soggetti interni o esterni"* (Sarathy, 2005; Daschkovska, 2010). È importante quindi il controllo degli accessi nei terminal e nei porti. Solitamente i

terminal e i luoghi di sosta delle ILU sono i punti della filiera in cui si manifesta maggiore vulnerabilità (Crist et. al., 2005; Strategic Forecasting Inc., 2006). Gli strumenti che vengono utilizzati vengono ricondotti alla categoria di *"Facility Management"* (paragrafo 3.2.1).

Persone

Il principale problema è quello di assicurarsi che tutto il personale che entra in contatto con il container sia fidato (Sarathy 2005). Spesso rimane una questione aperta, considerando i limiti imposti dalle normative sulla privacy presenti in molti Paesi (Sarathy and Robertson, 2003), i quali impediscono alle aziende di ottenere informazioni complete riguardo al personale. Gli strumenti di sicurezza che agiscono a favore dell'affidabilità del personale vengono ricondotti alla categoria di *"Human Resource Management"* e *"Awareness Management"* (paragrafi 3.2.7 e 3.2.8).

Informazioni

L'affidabilità e le performance di una supply chain dipendono fortemente dalla raccolta e dall'elaborazione di informazioni accurate. L'obiettivo è quello di "*prevenire accessi non autorizzati ai dati per evitare possibili alterazioni e per falsificare i manifesti del carico, oppure per salvaguardare le informazioni"* (Sarathy, 2005). Spesso i furti e le manipolazioni vengono compiuti da persone che hanno ottenuto informazioni privilegiate fornite da parte di chi entra in contatto con il carico (operatori del terminal, trasportatori) (Daschkovska, 2010). Gli strumenti di sicurezza delle informazioni si riferiscono alla categoria di "*Information Management System*" (paragrafo 3.2.5).

2.5 Criticità dell'approccio alla sicurezza

In seguito agli attacchi dell'11 settembre, come discusso precedentemente le organizzazione hanno prestato maggiore attenzione alle tematiche di SCS. Tuttavia, una ricerca condotta nel 2005 da Wilson, dimostra che, nonostante gli sforzi congiunti di Enti governativi e imprese (che a partire dal 2001 si sono concretizzati in numerose iniziative pubbliche e private), la vulnerabilità all'interno delle supply chain nella maggior parte dei casi non è stata eliminata o diminuita in maniera significativa. Williams et al. (2008) trovano una spiegazione al risultato di questa ricerca: *"la primaria questione all'interno della SCS è che le organizzazioni non conoscono l'efficacia delle loro pratiche fino a che non vengono applicate sul campo"*. Inoltre, aggiungono che un altro problema è la scarsa propensione che alcune organizzazioni

hanno verso l'approccio di risk management e le difficoltà nel pensare ad un approccio inter-organizzativo di SCS. Ricerche successive, in riferimento a quest'ultima criticità, dimostrano tuttavia la crescente diffusione di applicazioni e procedure sviluppate per certificare partner nella global supply chain e per educare i partner a credere nell'efficacia della filosofia della SCS. In ogni caso l'utilizzo di alcune tecnologie particolarmente efficaci in termini di sicurezza ed efficienza (ad esempio tecnologie per lo scanning di container) viene ostacolato dagli utilizzatori finali perché non è chiara l'assegnazione di responsabilità, dei benefici e dei costi da sostenere per la formazione e l'applicazione di questi strumenti tra i vari attori della filiera (IMCOSEC 2010).

Il progetto IMCOSEC inoltre, nasce per cercare di risolvere un'ulteriore criticità riscontrata negli approcci di SCS, ossia la mancanza di un approccio alla sicurezza integrato, che coinvolga l'intera supply chain considerando il flusso di ILU dall'origine a destino, e considerando tutti i possibili eventi di rischio che possono manifestarsi in ogni singolo punto debole della supply chain. In IMCOSEC si afferma che *"è ampiamente accettato che la sicurezza al 100% della catena intermodale non è raggiungibile. La sicurezza rimane comunque vulnerabile alle classiche minacce come furti, contrabbando o contraffazione tanto quanto alle "nuove" minacce di attacchi terroristici. Tuttavia è possibile migliorare la sicurezza della supply chain totale, migliorando il livello di sicurezza nei punti deboli della catena, tramite un approccio integrato".*

In definitiva, la mancanza di conoscenza delle misure di sicurezza, la scarsa preparazione sul tipo di minacce e i trade-off che sono emersi dall'analisi delle prestazioni organizzative, aumentano significativamente la diffidenza da parte dei manager verso le pratiche di SCS e la conseguente difficoltà nel mettere al sicuro le supply chain.

2.6 Conclusioni

Come abbiamo visto nel capitolo, il termine sicurezza non ha una definizione univoca e le tematiche ad essa associate possono essere trattate dalle aziende sotto diversi punti di vista in base all'ambito a cui si riferiscono o all'approccio utilizzato. Abbiamo visto come il concetto di sicurezza all'interno delle organizzazioni si sia anche evoluto nel corso degli anni, trovando la massima espressione nelle pratiche di Supply Chain Security. In seguito agli attacchi terroristici dell'11 settembre 2001 si è assistito al

cambiamento del modo di operare delle organizzazioni di tutto il mondo generando una nuova consapevolezza verso le tematiche di sicurezza. Ci siamo focalizzati sulle pratiche di SCS collocandole all'interno delle strategie di mitigazione del rischio, in ambito di Risk Management, evidenziando quanto sia importante l'analisi dei rischi che le supply chain corrono: infatti, solo tramite un'analisi accurata dei rischi è possibile capire le strategie di sicurezza da applicare per ridurre la vulnerabilità delle supply chain. In questo senso, è possibile agire su due determinanti della vulnerabilità, ossia la probabilità di accadimento di una disruption e la severità delle conseguenze, le quali determinano la prestazione di sicurezza, che può essere dettagliata in termini di sicurezza preventiva e di resilienza. Rimanendo nel tema delle prestazioni, abbiamo visto come le strategie di SCS possano impattare anche su altre performance organizzative, quali trasparenza, efficacia ed efficienza. In particolare ci siamo soffermati sulla relazione tra le prestazioni di sicurezza e di efficienza, in quanto possono risultare in trade-off, se osservate in condizioni operative normali. Abbiamo inoltre focalizzato le nostre ricerche sulla sicurezza in relazione alla filiera del trasporto intermodale, definita ILU Supply Chain, essendo le ILU soggette ad attacchi di tipo terroristico, furti, contrabbando e manipolazioni di ogni genere. In particolare siamo andati ad analizzare i punti deboli della ILU supply chain. Infine sono emerse alcune criticità rilevanti che spiegano perchè ancora oggi la sicurezza delle supply chain non abbia raggiunto risultati significativi. Anzitutto manca una corretta comunicazione delle pratiche di SCS e dei benefici ottenibili, oltre a non esserci ricerche quantitative che dimostrino gli impatti positivi verso entrambe le prestazioni di efficienza ed efficacia. Manca inoltre una cultura di gestione del rischio che non permette alle organizzazioni di avere ben chiari i rischi che corrono e quindi fa mancare il presupposto fondamentale per la riduzione della vulnerabilità. A queste criticità si aggiungono la mancanza di un approccio alla sicurezza integrato di filiera e la presenza di trade-off tra le prestazioni di sicurezza ed efficienza a rallentare la diffusione di strategie di SCS.

Nel capitolo successivo vedremo più nel dettaglio con quali strumenti si possono concretizzare le strategie di SCS.

3 Analisi della letteratura

L'obiettivo di questo capitolo è approfondire la letteratura riferita alla supply chain security con focus sugli strumenti[10] necessari alle aziende per incrementare la sicurezza. Inizialmente abbiamo analizzato i principali programmi obbligatori e volontari che a livello internazionale sono stati proposti per aumentare la sicurezza delle supply chain.
Abbiamo quindi proseguito classificando tutti gli strumenti emersi dallo studio della letteratura e dei programmi di sicurezza, studiandone l'utilizzo e le modalità di applicazione. Fornito il quadro generale dei mezzi a disposizione delle aziende per aumentare la sicurezza della propria catena di fornitura abbiamo effettuato un'analisi di densità sulle famiglie di strumenti per evidenziare quali siano quelle meno approfondite in letteratura per mettere in luce gli ambiti meno sviluppati. A questa analisi è stata affiancata una ricerca in letteratura sugli impatti diretti che gli strumenti hanno sulle prestazioni organizzative, per differenziare meglio le categorie di strumenti.

3.1 Principali programmi di sicurezza per le supply chain

Numerose tipologie di risposte sono state intraprese negli ultimi decenni per migliorare la sicurezza delle supply chain. Queste variano da programmi operativi specifici per un singolo paese fino a proposte di soluzioni e standard a livello globale.
Tutte queste iniziative, secondo Gutierrez e Hintsa (2006), possono essere classificate rispetto ai seguenti parametri:

- Tipologia di attore all'origine (organizzazione internazionale, agenzia governativa, autorità di trasporto, amministrazioni doganali, settore privato)
- Modalità di trasporto (mare, aria, strada, ferrovia, canali navigabili interni)
- Tipologia applicazione (volontaria, obbligatoria)
- Obiettivi principali (aumento capacità di controllo delle autorità doganali, riduzione di vulnerabilità geografiche/industriali, sviluppo di standard globali, sviluppo di programmi pilota/tecnologie)

[10] Il termine "strumento" è usato in senso figurato, per esprimere "ciò di cui ci si serve per ottenere qualcosa" (definizione da dizionario della lingua italiana) che in questo caso corrisponde alla supply chain security. Considereremo come strumenti, quindi, sia device fisici che pratiche gestionali

Dopo gli eventi dell'11 Settembre le autorità governative hanno spinto verso un nuovo approccio per iniziative rivolte alle supply chain, che ponessero maggiore attenzione alla security. Le più significative hanno portato alla definizione di protocolli per il tracking e lo screening dei cargo, che dall'America si sono diffuse in tutto il mondo; attualmente questi protocolli sono compresi nei principali programmi di sicurezza internazionali. Gli eventi dell'11 Settembre hanno avuto anche un altro effetto; come rilevano Donner e Kruk (2009) "*prima degli eventi, il focus degli enti governativi era sull'agevolazione del commercio e l'armonizzazione delle regole e pratiche di commercio, in conseguenza delle norme ambientali e commerciali imposte dalla Convenzione di Kyoto. Dopo l'11 Settembre si ebbe un notevole mutamento che spinse verso l'aumento delle misure anti-terroristiche e di security. Per quanto riguarda la security, infatti, prima dell'11 Settembre le autorità erano principalmente responsabili del controllo sulla merce importata, che presupponeva la verifica dei documenti di accompagnamento, e quando necessario, l'ispezione fisica della merce. In aggiunta, il focus delle pratiche svolte nel settore privato era limitato all'interno dell'azienda. Questo approccio è stato ora superato e arriva alla sicurezza dell'intera supply chain. Infine, viste le minacce che diventano sempre più globali, e visto le sempre più forti interdipendenze nel mondo del commercio, il precedente focus limitato ad un'area geografica è stato espanso ad un approccio globale".*

Come abbiamo visto nel paragrafo 2.3.2, la sicurezza della supply chain è quindi passata dall'essere una preoccupazione pubblica o privata, all'essere un obiettivo comune pubblico/privato. La nuova filosofia d'azione prevede di raggiungere la messa in sicurezza della supply chain in maniera efficace ed efficiente dal punto di vista economico; si prevede inoltre di aumentare le sinergie tra settore pubblico e privato.

A questo proposito, negli ultimi anni alcuni enti governativi hanno stabilito delle regole vincolanti da seguire per le varie tipologie di attori delle supply chain. Queste iniziative obbligatorie, rappresentano però una piccola parte delle misure di sicurezza potenzialmente applicabili per la messa in sicurezza del trasporto globale delle merci.

In Tabella 9 vengono riportate le iniziative obbligatorie più significative, classificate rispetto alle dimensioni individuate da Gutierrez e Hintsa (2006).

Tabella 9: Classificazione dei programmi obbligatori di sicurezza

Nome/anno di inizio	Paese di origine dell'istituto	Modalità	Partecipanti	Categoria	Obiettivo
24 Hour Rule, 2003	US	Trasporto via mare	Porti US	Governativa obbligatoria	Informazioni avanzate
ISPS, 2004	IMO	Trasporto via mare	167 Stati membri	Internazionale obbligatoria	Standard e framework per la valutazione del rischio
Pre-arrival & Pre-departure EU, 2009-2011	EU	Trasporto via mare	Stati dell'UE	Obbligatoria	Informazioni avanzate
Japan ACI, 2007	Giappone	Trasporto via mare e aria	Porti e aeroporti giapponesi	Governativa obbligatoria	Informazioni avanzate
Mexico 24 Hour Rule, 2007	Messico	Trasporto via mare	Porti messicani	Governativa obbligatoria	Informazioni avanzate
10+2, 2009	US	Tutte	Porti US	Governativa obbligatoria	Informazioni avanzate
China 24 Hour advanced manifestation Rule, 2009	Cina	Trasporto via mare	Porti cinesi	Governativa obbligatoria	Informazioni avanzate
100% scanning, 2012	US	Trasporto via mare	Programma pilota (5 porti US)	Internazionale obbligatoria	Supply chain security

Maggiormente significative dal punto di vista delle implicazioni pratiche, sono i programmi di sicurezza con applicazione volontaria, classificate nella Tabella 10 rispetto alle dimensioni individuate da Gutierrez e Hintsa (2006).

Tabella 10: Classificazione dei programmi volontari di sicurezza

Nome/anno di inizio	Paese di origine dell'istituto	Modalità	Partecipanti/ stato	Categoria	Obiettivo
TAPA, 1997	US	Trasporto su gomma	207 membri	Privata volontaria	Report incidenti criminali/identificazione soluzioni/condivisione informazioni
C-TPAT, 2001	US	Tutte	6375 certificazioni e 3916 aziende approvate	Governativa volontaria	Supply chain security
CSI, 2002	US	Trasporto via mare	58 porti	Governativa volontaria	Supply chain security
WCO SAFE FoS, 2005	WCO	Tutte	156 Stati membri	Internazionale volontaria	Standard per la supply chain security e per l'agevolazione del commercio
ISO 28000, 2005	Comitato tecnico ISO	Tutte	157 Paesi membri	Internazionale volontaria	Supply chain security
EU-AEO, 2008	Commissione Europea	Tutte	192 aziende	Governativa volontaria	Supply chain security e agevolazione del commercio

Questi programmi possono condividere obiettivi e metodologie, e in alcuni casi presentano delle sinergie se applicati congiuntamente.

Transported Asset Protection Association (TAPA)

TAPA è un programma nato da un'associazione no profit nel 1997 in USA, e diffusosi in Europa dal 1999 e in Asia dal 2000. Il programma è nato dopo un periodo di crescita di furti e crimini negli Stati Uniti e dopo la nascita del mercato unico europeo (con conseguenti facilitazioni di movimento all'interno dell'UE).

La mission del programma è di *"proteggere gli asset dell'industria high-tech nella supply chain con:*

- *condivisione di informazioni su base globale;*
- *cooperazione per una sicurezza preventiva;*
- *incremento del sostegno da parte delle aziende logistiche e di trasporto e, dove possibile, delle forze dell'ordine e degli enti governativi."*[11]

Il programma è quindi rivolto alla protezione del trasporto di merce ad alto valore da potenziali minacce intenzionali; l'obiettivo ultimo è quello di identificare le situazioni che hanno causato dei buchi di sicurezza nel passato e diffondere informazioni sulle routine e procedure da mettere in atto per evitare il ripetersi di queste situazioni. Il programma è rivolto ad aziende di media/grande dimensione che effettuano un trasporto stradale o combinato strada/ferrovia.

Operativamente TAPA aiuta a combattere la criminalità che attacca il trasporto merci tramite:

- "*i requisiti di sicurezza predisposti dall'Associazione che sono riconosciuti nel mondo come standard industriali da seguire per la sicurezza dei magazzini, dei centri logistici e per la sicurezza dei trasporti di merce;*
- *il servizio di informazione sugli incidenti occorsi (TAPA Incident Information Service) che cataloga costantemente e condivide dati ed informazioni; questo permette di poter conoscere tempestivamente le novità sulle tecniche criminali utilizzate per attaccare le merci, di evitare zone e predisposizioni rivelatesi pericolose, di proteggere le merci durante il trasporto e, se richiesto, anche di dare informazioni e rintracciare i beni rubati;*
- *la condivisione di informazione dei livelli dei dipartimenti governativi più importanti, delle agenzie di sicurezza e delle forze di polizia internazionali. TAPA sostiene le necessità dei propri membri nella loro campagna alla riduzione degli attacchi della criminalità;*

[11] www.tapaemea.com

- *le conferenze trimestrali tenute nell'area EMEA (Europa, Medio Oriente, Africa) che riuniscono più di 150 professionisti della sicurezza, i quali ascoltano presentazioni sulle ultime soluzioni nella lotta agli attacchi della criminalità, condividono tecniche e pratiche e si relazionano con altre aziende e persone;*
- *i bollettini di informazione mensili".* [12]

Le iniziative più importanti del programma riguardano quindi il servizio di informazione sugli incidenti occorsi e gli standard di sicurezza minimi richiesti alle aziende per poter aderire al progetto, che includono strumenti di sicurezza fisica delle ILU e routine di sicurezza standard.

Customs-Trade Partnership Against Terrorism (C-TPAT)

Il programma C-TPAT è nato da uno sforzo condiviso del governo statunitense e delle aziende importatrici di beni negli Stati Uniti che, dopo gli eventi dell'11 Settembre, hanno convenuto che la sicurezza doganale sarebbe stata molto maggiore se anche le aziende private fossero state coinvolte nel processo di controllo e ispezione dei cargo.

Questo approccio alla sicurezza è rivolto principalmente alla protezione da atti terroristici rivolti alla supply chain, con focus sulla sicurezza dei contenitori.

Attualmente il programma C-TPAT è rispettato dalla maggior parte delle aziende che importa beni negli Stati Uniti (più di 10.000 aziende[13]) includendo trasportatori, intermediari, produttori e importatori.

La strategia del programma prevede un approccio su più livelli che deve:

- assicurare che i partner C-TPAT migliorino la sicurezza della propria supply chain rispettando i criteri di sicurezza imposti dal programma;
- fornire incentivi e benefici che includono processi più veloci di spedizione/ricezione tra membri C-TPAT;
- internazionalizzare i principi chiave del programma C-TPAT tramite cooperazione e collaborazione con le comunità internazionali;
- supportare le agenzie doganali;
- migliorare la gestione del programma C-TPAT stesso.

Il programma prescrive una lista di procedure, processi e tecnologie di cui ogni azienda si deve dotare per consentire la messa in sicurezza dei contenitori durante i processi di

[12] www.tapaemea.com
[13] www.c-tpat.com

imballaggio, manipolazione, tracciatura e distribuzione, entrando anche nei particolari di adozione e implementazione delle stesse.

I membri del C-TPAT per essere certificati devono verificare che anche i propri partner, subcontractor e fornitori rispettino i requisiti di sicurezza minimi richiesti; in caso un'ispezione rilevi una non conformità, la certificazione viene tolta e l'azienda dovrà sottoporsi ad una nuova procedura di certificazione. Seppur rivolta ad aziende che importano prodotti negli Stati Uniti, la certificazione C-TPAT è molto utilizzata anche dalle aziende che non hanno traffici negli USA.

I benefici dell'adesione volontaria al programma sono i seguenti:

- riduzione delle ispezioni doganali;
- commercio libero e sicuro;
- maggiore resilienza (in caso di disruption);
- accesso privilegiato al carico/scarico;
- marketing (reputazione e brand);
- lotta al terrorismo (prevenzione).

Tra questi benefici, tralasciando le misure preventive, il più apprezzato da parte delle aziende è la maggior velocità nelle pratiche doganali.

"I membri C-TPAT subiscono minori ispezioni di sicurezza; gli importatori C-TPAT hanno il 60% di probabilità in meno di incorrere in un'ispezione e il 40% di probabilità in meno di incorrere in una verifica di conformità".[14]

Container Security Initiative (CSI)

Il programma CSI è stato istituito nel 2001 e si focalizza sulla messa in sicurezza del commercio globale legato ai contenitori marittimi, rivolgendosi ai paesi che devono esportare negli Stati Uniti. Questi paesi sono invitati a instaurare una cooperazione con la CBP (US Custom and Border Protection) per assicurare che tutti i container ad alto rischio di azioni terroristiche siano individuati ed ispezionati prima del carico sulla nave con destinazione Stati Uniti. Il programma CSI si occupa quindi di effettuare uno screening preventivo dei container e di sviluppare delle azioni investigative aggiuntive per assicurare la sicurezza del cargo. L'obiettivo è far diventare i *"porti statunitensi di destino come l'ultima linea di difesa, non la prima"*.[15] Il dipartimento della difesa

[14] Citazione del CPB (Custom and Border Protection) estrapolata da "Supply chain security guide", 2009
[15] Citazione del CPB (Custom and Border Protection) estrapolata da "Supply chain security guide", 2009

statunitense ritiene che questo regime di sicurezza promosso dal CSI completi in maniera efficace le direttive del C-TPAT.

Operativamente l'individuazione dei container ad alto rischio viene effettuata mediante l'utilizzo di tecnologie a raggi X e a radiazioni. I paesi che decidono di aderire al programma devono quindi dotarsi di tecnologie per effettuare ispezioni del container non intrusive; per garantire l'integrità del container durante il trasporto fino al porto di destino vengono applicati sigilli meccanici o elettronici.

Il programma inoltre richiede l'instaurazione di una relazione collaborativa con gli stati membri, che prevede condivisione di informazioni, best practise e trend locali, e l'implementazione di un meccanismo di scambio informativo automatizzato. Le collaborazioni diventano utili nella gestione di situazioni ad alto rischio, e nel ristabilire il flusso commerciale tradizionale dopo una disruption, con conseguente aumento della resilienza della supply chain.

World Customs Organization SAFE Framework of Standards (WCO SAFE FoS)

Dal Giugno 2005 i membri del WCO hanno iniziato ad implementare le procedure "SAFE Framework of Standards to secure and facilitate global trade".

Il framework si propone di:

- stabilire standard per portare sicurezza nelle supply chain e per promuovere certezza e prevedibilità;
- permettere la gestione integrata della supply chain per ogni modalità di trasporto;
- sviluppare il ruolo, le funzioni e le capacità degli enti doganali affinchè si colgano le opportunità e le sfide del ventunesimo secolo;
- rafforzare la cooperazione tra gli enti doganali e le amministrazioni per migliorare la capacità di individuare consegne ad alto rischio;
- rafforzare la cooperazione tra aziende ed enti doganali;
- promuovere la circolazione continua e sicura di merci nelle supply chain internazionali.

Il programma è costituito da quattro elementi principali. Il primo riguarda la standardizzazione dei requisiti per le spedizioni in entrata, in uscita ed in transito.

Il secondo impone agli stati membri di implementare un consistente approccio di risk management per affrontare le minacce di sicurezza. Il terzo elemento richiede agli

esportatori di effettuare ispezioni sulla merce in uscita (sulla base delle richieste del CSI); mentre l'ultimo definisce i benefici per gli enti doganali che forniscono i minimi standard di sicurezza imposti e per chi effettua best practise.
Gli standard WCO forniscono un modello per l'implementazione di una politica di sicurezza da diffondere a livello internazionale, ma anche nazionale e regionale.
A livello mondiale, la consapevolezza e la preparazione degli enti doganali è molto diversa; per questo motivo la diffusione degli standard minimi rimangono non uniformi, nonostante le iniziative di training su larga scala promosse dal WCO.

ISO 28000

Gli standard ISO 28000 si riferiscono a sistemi per la gestione in sicurezza di una supply chain; possono essere applicati a livello internazionale e adattabili a tutte le rotte e le tipologie di trasporto. Come affermano Donner e Kruk (2009) a proposito di questa tipologia di standard *"l'idea di base riguarda il miglioramento del controllo sul flusso del trasporto, per combattere il contrabbando, per rispondere alle minacce terroristiche e di pirateria, e per creare un approccio alla gestione sicura di una supply chain internazionale"*.
Nello specifico l'approccio include aspetti finanziari, produttivi, di gestione delle informazioni, di imballaggio, di immagazzinamento e di trasporto dei prodotti. L'approccio prevede di:

- stabilire, implementare, mantenere e sviluppare un sistema di gestione della sicurezza;
- assicurare la conformità rispetto alle politiche gestionali previste;
- poter dimostrare tali conformità ad altri ;
- far certificare il sistema di gestione della sicurezza da un ente terzo accreditato oppure fare un'auto-dichiarazione di conformità alla ISO 28000.

Il processo ISO 28000 si basa sul classico schema "Plan – Do – Check – Act" e offre metodologie pratiche d'implementazione di best practise.
L'obiettivo ultimo dello standard ISO 28000 è l'agevolazione del commercio internazionale e l'incremento dell'abilità di un'organizzazione ad'individuare vulnerabilità strategiche e operative. Lo standard prevede un processo di controllo e miglioramento continuo.

EU Authorized Economic Operator (AEO)

Un AEO è una *"parte coinvolta nel traporto internazionale di beni, in qualsiasi ruolo approvato da o per conto di un ente doganale come conforme agli standard di sicurezza del WCO o equivalenti".*[16]

Il programma AEO è stato promosso dalla Commissione Europea con lo scopo di individuare degli operatori di trasporto affidabili che possano usufruire di agevolazioni nel commercio.

I benefici della certificazione AEO sono notevoli: il rilascio anticipato dei documenti di trasporto, la riduzione dei transit time, l'accesso a procedure speciali durante periodi nei quali si sono verificare disruption o alti livelli di minacce e priorità durante le ispezioni dei contenitori.

Nella procedura di certificazione, le aziende devono aderire ad un set standard di procedure di sicurezza e implementare best practise che garantiscano la salvaguardia dell'integrità del contenitore in tutto il processo di trasporto, fino all'ente doganale di destino.

L'auto-valutazione prevede:

- best practise predeterminate incluse nell'attuale processo di trasporto;
- validazione del processo effettuata da un ente doganale riconosciuto;
- adozione delle tecnologie più moderne per salvaguardare l'integrità dell'ILU;
- comunicazione aperta con le autorità doganali per ricevere gli aggiornamenti degli standard di sicurezza e delle best practise.

3.2 Classificazione degli strumenti di sicurezza

Per classificare gli strumenti per aumentare la SCS ci siamo basati sull'analisi dei principali programmi di sicurezza per supply chain e della letteratura su questo tema. Abbiamo condotto l'analisi principalmente sulle banche dati "ISI Web of Knowledge"," Scopus", "Emerald" e "Google Scholar" ricercando le parole chiave "supply chain security". Abbiamo selezionato 25 tra articoli, journal, tesi e pubblicazioni degli ultimi 10 anni che meglio rispecchiavano i criteri di ricerca immessi e l'ambito del nostro lavoro di tesi (trasporto intermodale strada/ferrovia), e basandoci su questi abbiamo effettuato la classificazione degli strumenti.

[16] Definizione del WCO

I maggiori programmi di certificazione, così come gli autori che hanno affrontato questa tematica, approcciano l'argomento con livello di dettaglio e obiettivi differenti. Di conseguenza anche la variabilità nelle classificazioni proposte è molto alta; alcuni programmi e autori prescrivono una lista dettagliata delle procedure e attività da seguire, oltre alle tecniche di controllo e alle tecnologie da implementare per ottenere performance sicure. Altri si limitano a fornire una serie di "Security Must" e obiettivi da raggiungere senza prescrivere dettagliatamente le procedure d'implementazione.

In ogni caso è possibile individuare dei temi comuni. Nello specifico la classificazione proposta di seguito vuole evidenziare le analogie dei principali programmi di certificazione volontaria precedentemente descritti nel paragrafo 3.1.

La Figura 38 riporta il livello "macro" di classificazione, che individua le categorie degli strumenti di SCS.

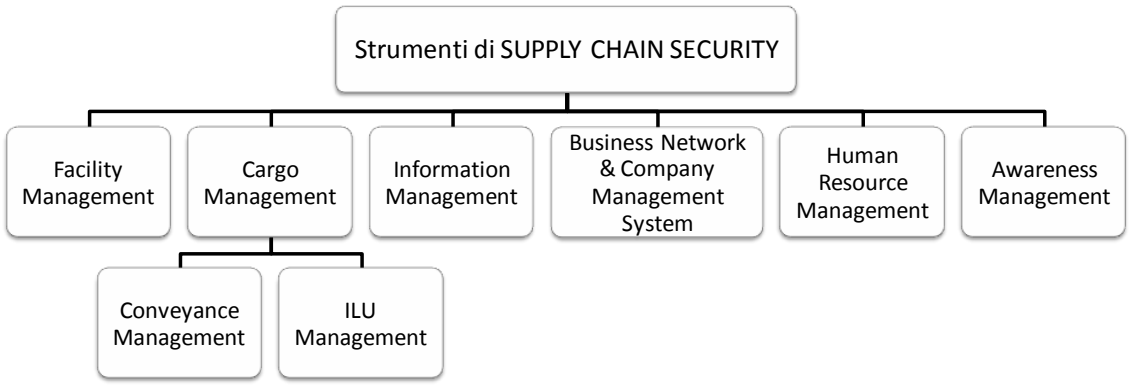


Figura 38: Classificazione ambiti SCS

Dalla Tabella 12 alla Tabella 19 sono evidenziati tutti i legami tra gli strumenti e le fonti bibliografiche che li hanno ritenuti importanti per incrementare il livello di sicurezza della supply chain.

Tabella 11 : Legenda

	Fonte bibliografica
(1)	Sheffi Y. (2001) - "Supply chain management under the threat of international terrorism", International Journal of Logistics Management (v12, no. 2)
(2)	Knight P. (2003) – "Supply chain security guidelines", IBM Corporation
(3)	Northland Insurance (2003) – "Vehicle & Cargo theft"
(4)	Rice J.B., Caniato F. (2003) - "Building a secure and resilient supply chain", Supply Chain Management Review (Ottobre/Novembre)
(5)	Motorola (2004) - "The opportunities for active RFID in container shipping"
(6)	Willis H., Ortiz D (2004) – "Evaluating the security of the global containerized supply chain", Technical report of RAND Corporation

(7)	Harrald J., Stephens H.W., van Dorp J.R. (2004) – "A framework for sustainable port security", Journal of Homeland Security and Emergency Management (v1,issue 2, article 12)
(8)	Closs D., McGarrel E. (2004) – "Enhancing security throughout the supply chain", Special report series of IBM Center for the business of Government
(9)	Sheffi Y.(2005) - "Weathering the storm", The business review for procurement leaders
(10)	Benson S. (2005) – "The role of organizational culture in creating secure and resilient supply chains", Degrees of Master of Science in Transportation and Master of Engineering in Logistics, MIT
(11)	Purtell D. (2006) – "Is it safer?", Cargo Security International (Ottobre/Novembre 2006)
(12)	Stratfor inc.(2006) - "Cargo theft: from silent crime to violent crime?"
(13)	Downey L. (2006) – "International Cargo Conudrum", RFID Journal
(14)	Gutierrez X., Hintsa J. (2006) – "Voluntary supply chain security programs: a systematic comparison", Cross-border Research Association, Losanna
(15)	U.S. Custom and Border Protection (2006) – "Supply Chain Security best practice. C-TPAT"
(16)	van Oosterhout M., Veenstra A.W., Meijer G., Popal N., van den Berg J. (2006) – "Visibility Platforms for Enhancing supply cahin security: a case study in the port of Rotterdam", International Symposium on Maritime Safety, Security and Environmental Protection, Atene
(17)	Purtell D., Rice J.B. (2007) – "Assessing cargo supply risk", Security Management Magazine Online
(18)	Werner S., Schuldt A., Daschkovska K. (2007) - "Agent-based container security systems: an interdisciplinary perspective", TZI University Brema, BIBA University Brema
(19)	Gould J. (2007/2008) - "Supply chain security: an overview of theoretical applications", Research report 2007/2008 of IGSDL (pp. 26-28)
(20)	Daschkovska K., Scholz-Reiter B. (2008) – "Electronic Seals for Efficient Container Logistics", BIBA University Brema, IGSDL University Brema
(21)	Williams Z., Lueg J.E., LeMay S. (2008) – "Supply chain security: an overview and research agenda", The International Journal of Logistics Management (Vol. 19 No. 2, pp. 254-281)
(22)	Donner M., Kruk C. (2009) - "Supply chain security guide", Department for International Development
(23)	Nassimbeni G. (2009) – "Il problema della vulnerabilità delle moderne reti internazionali", Logistica Management (Dicembre 2009, pp. 19-22)
(24)	Urciuoli L. (2009) – "Supply chain security. Mitigation measures and a logistics multi-layered framework", Department of Industrial Management and Logistics, Lund University
(25)	Kim S.J., Deng G., Gupta K.S. (2009) - "Enhancing cargo container security during transportation: a mesh networking based approach", Arizona State University, Tempe (Arizona)

Tabella 12: Fonti bibliografiche (2001-2006) per Facility Management e Conveyance Management

		ARTICOLI 2001 - 2006												
MACRO	STRUMENTO	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)
FACILITY MANAGEMENT	guarded gate		■	■	■			■						
	lighting		■	■										
	clearly marked control areas		■					■	■					
	establish driver waiting areas													
	specific equipment for key operational/high-value cargo areas		■					■	■					
	minimization of exit/entry point													
	fence		■	■	■			■	■					
	locks		■					■	■					
	wall		■					■	■					
	closed circuit television		■	■	■				■					
	alarm system		■						■					
	surveliance				■		■	■	■					
	acces control system (person and vehicles)		■	■	■		■	■	■		■			
	identification system (person and vehicles)		■				■	■	■		■			
CONVEYANCE MANAGEMENT	inspecting conveyance in route and in handling point		■					■	■			■		
	RFID system	■	■		■	■	■	■	■			■	■	■
	barcode & scanning cards	■	■		■		■	■	■			■	■	■
	Supply Chain Event Management (SCEM)		■					■	■			■	■	■
	wireless sensor network		■		■			■	■			■	■	■
	tracing cargo with driver data port		■					■	■			■	■	■
	GPS	■	■	■	■	■	■	■	■			■	■	■
	security escorts to and from the port		■					■	■			■		
	vehicle immobilisation device													
	green lanes													■
	avoid travelling through high-risk areas			■										
	avoid parking in high-risk areas		■	■					■					
	avoid stops en route			■										
	route security system	■	■	■			■		■					

Tabella 13: Fonti bibliografiche (2006-2009) per Facility Management e Conveyance Management

		ARTICOLI 2006 - 2009											
MACRO	STRUMENTO	(14)	(15)	(16)	(17)	(18)	(19)	(20)	(21)	(22)	(23)	(24)	(25)
FACILITY MANAGEMENT	guarded gate		■	■					■			■	
	lighting	■	■	■					■	■		■	
	clearly marked control areas	■		■								■	
	establish driver waiting areas		■										
	specific equipment for key operational/high-value cargo areas			■									
	minimization of exit/entry point		■										
	fence	■	■	■	■				■	■		■	
	locks	■	■		■								
	wall	■	■		■								
	closed circuit television	■	■	■					■			■	
	alarm system	■	■									■	
	surveliance	■	■		■					■		■	
	acces control system (person and vehicles)	■	■	■	■				■	■		■	
	identification system (person and vehicles)		■	■	■				■			■	
CONVEYANCE MANAGEMENT	inspecting conveyance in route and in handling point	■	■		■				■		■	■	
	RFID system	■	■	■					■	■	■	■	■
	barcode & scanning cards	■	■						■		■	■	
	Supply Chain Event Management (SCEM)	■							■		■	■	
	wireless sensor network	■							■		■	■	■
	tracing cargo with driver data port	■	■						■		■	■	
	GPS	■		■					■	■	■	■	■
	security escorts to and from the port	■			■								
	vehicle immobilisation device	■										■	
	green lanes							■		■		■	
	avoid travelling through high-risk areas		■									■	
	avoid parking in high-risk areas		■									■	
	avoid stops en route											■	
	route security system	■		■	■								

Tabella 14: Fonti bibliografiche (2001-2006) per ILU Management e Information Management

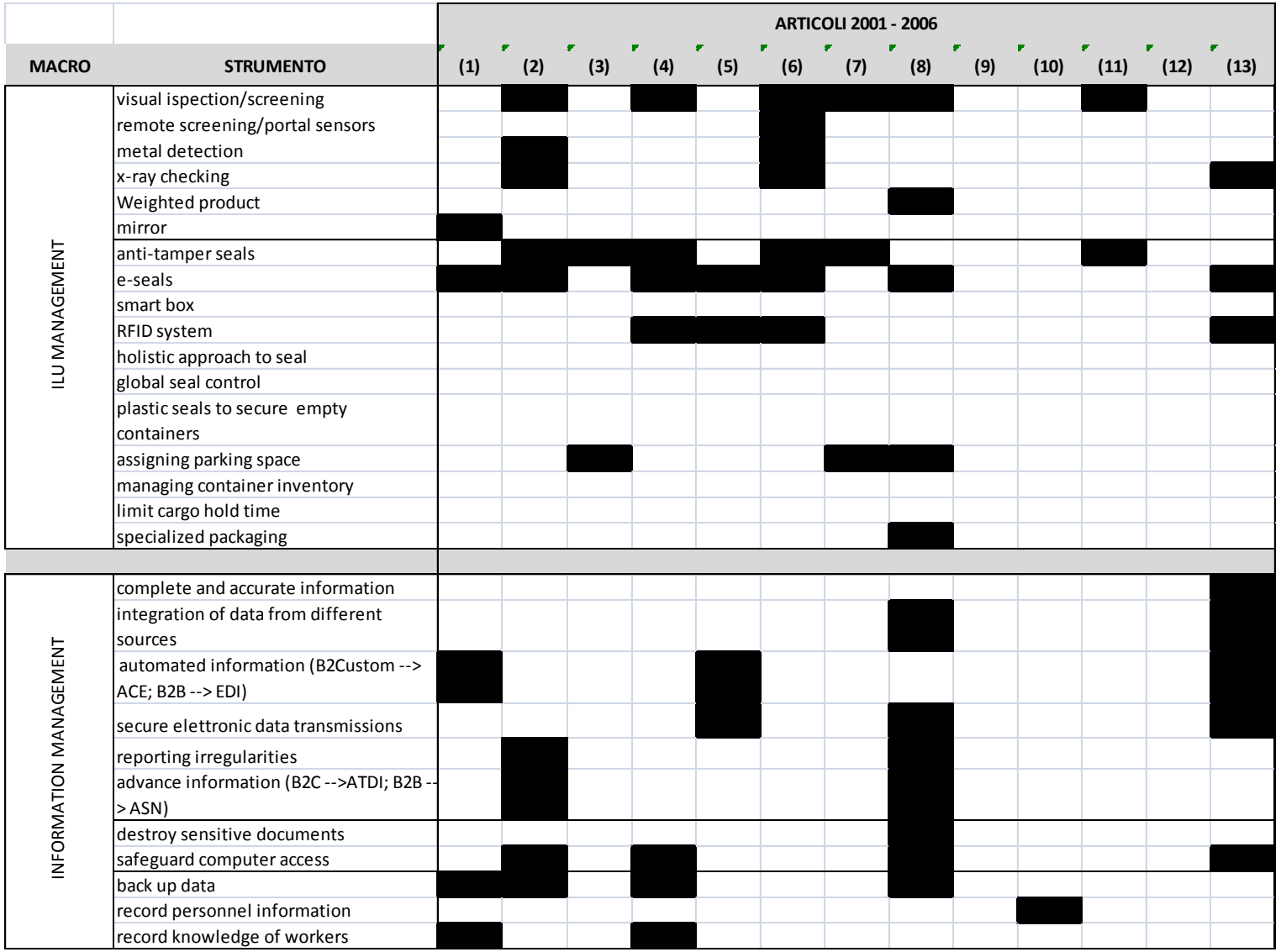


Tabella 15: Fonti bibliografiche (2006-2009) per ILU Management e Information Management

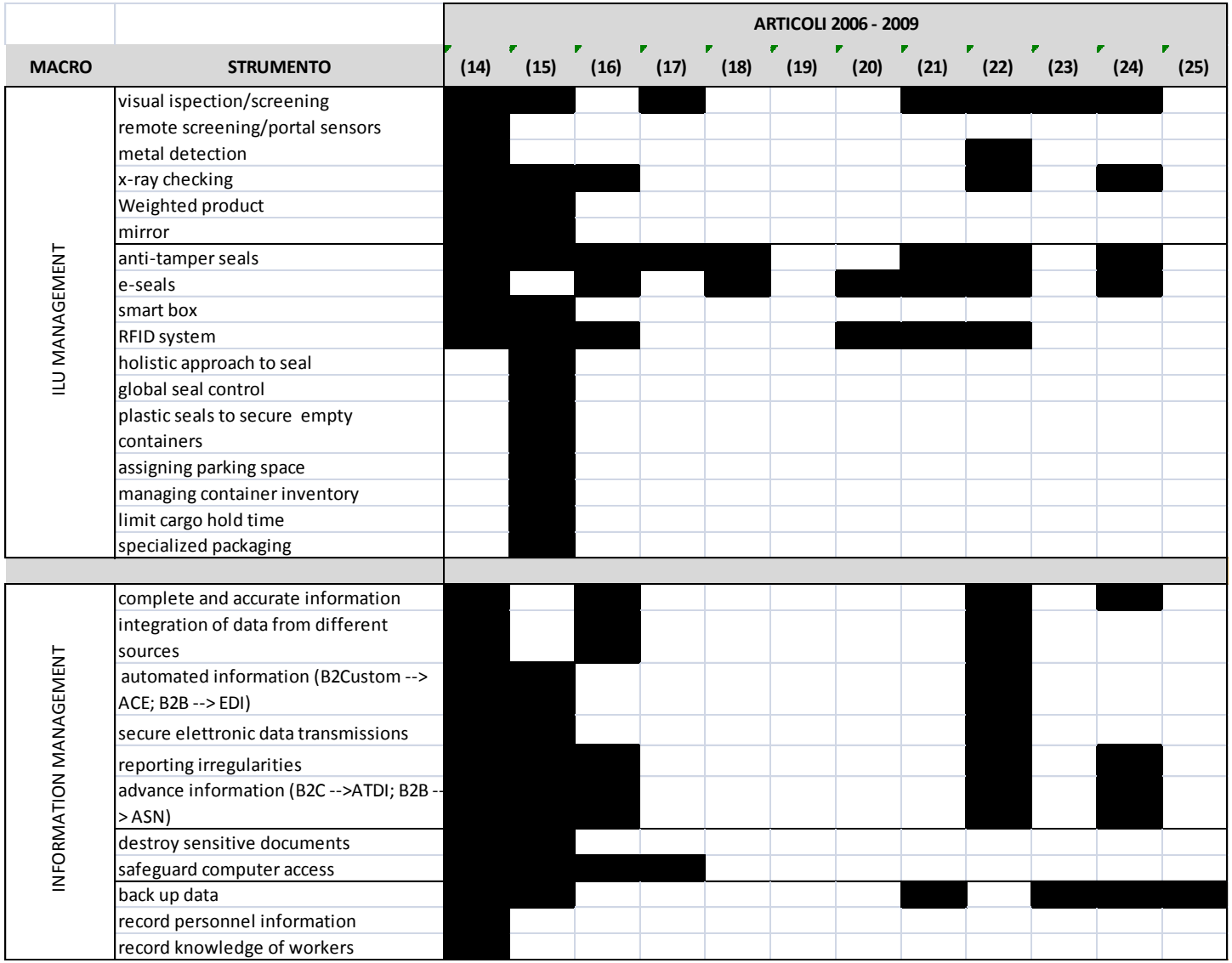


Tabella 16: Fonti bibliografiche (2001-2006) per Business Network & Company Management System

		ARTICOLI 2001 - 2006												
MACRO	**STRUMENTO**	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**(8)**	**(9)**	**(10)**	**(11)**	**(12)**	**(13)**
BUSINESS NETWORK & COMPANY MANAGEMENT SYSTEM	laws and certifications (ISO, AEO)	■			■		■			■	■	■		■
	std procedure	■	■		■		■	■	■	■	■			
	risk management		■		■			■	■	■	■	■		
	emergency plan (Business Continuity Planning, Crisis Management)	■	■		■		■	■	■	■	■			
	inventory management system (SS/ emergency stock)	■			■				■	■		■		
	monitor and synthesize information regarding security practise		■						■	■				
	alert system													
	security function/position (CSO)	■			■				■		■			
	total quality management	■							■	■				
	additional capacity	■			■		■		■	■				
	reconfigurable resource and planning				■					■				
	reconfigurable product									■				
	reconfigurable SC network	■			■					■				
	postponement	■								■				
	audits of partners' system security	■	■		■		■		■					■
	certifications (AEO, third-tier status)	■			■		■		■			■		■
	supplier base selection and reduction	■			■			■		■				
	integrated SC management	■						■	■	■	■			
	external comunication (feedback on requirements and performances)		■				■		■	■	■			
	inform government regarding known vulnerabilities	■	■				■		■	■				
	involves partners in setting security standards		■		■				■	■	■			
	sharing responsability	■	■						■	■				■

Tabella 17: Fonti bibliografiche (2006-2009) per Business Network & Company Management System

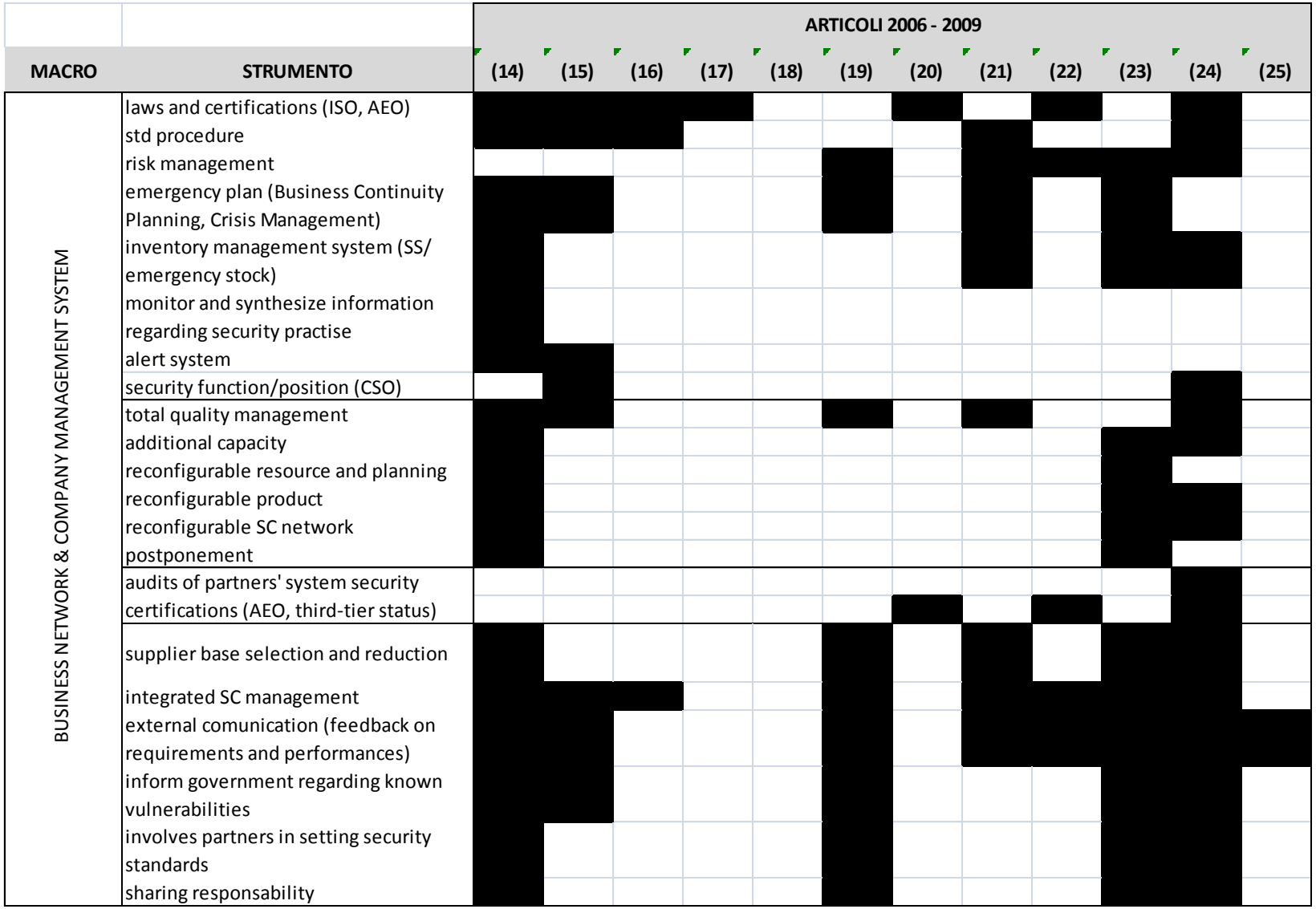


Tabella 18: Fonti bibliografiche (2001-2006) per Human Resource management e Awareness Management

MACRO	STRUMENTO	ARTICOLI 2001 - 2006 (1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)
HUMAN RESOURCE MANAGEMENT	background investigation on potential employees and third-party providers	■	■	■	■		■		■		■			
	interview/psychological examinations		■	■										
	hire security-specific skills										■			
	employee termination procedure													
	assign security responsabilities to personnel						■			■	■			
	rotating shipping/receiving personnel													
	multi-skilled workforce				■									
	estabilish security goals		■											
	measurement system of employee										■			
	incentive system for security		■						■		■			
AWARNESS MANAGEMENT	information dissemination process			■					■					
	contract with specific security requirements								■	■				
	simulations and excercises		■		■				■					■
	formal training		■	■	■				■		■			
	informal socialization				■						■			
	Security function/position (leadership)	■			■				■	■	■			
	involve outside expertees	■			■					■	■			
	total quality management	■								■				
	internal/external comunication				■					■	■			

Tabella 19: Fonti bibliografiche (2006-2009) per Human Resource management e Awareness Management

MACRO	STRUMENTO	ARTICOLI 2006 - 2009 (14)	(15)	(16)	(17)	(18)	(19)	(20)	(21)	(22)	(23)	(24)	(25)
HUMAN RESOURCE MANAGEMENT	background investigation on potential employees and third-party providers	■	■	■	■						■		
	interview/psychological examinations	■	■										
	hire security-specific skills		■										
	employee termination procedure	■	■									■	
	assign security responsabilities to personnel	■											
	rotating shipping/receiving personnel		■										
	multi-skilled workforce										■		
	estabilish security goals	■	■										
	measurement system of employee												
	incentive system for security	■	■	■									
AWARNESS MANAGEMENT	information dissemination process	■	■		■				■		■	■	
	contract with specific security requirements	■	■		■		■		■		■	■	
	simulations and excercises	■	■		■				■		■		
	formal training	■			■						■		
	informal socialization												
	Security function/position (leadership)		■								■	■	
	involve outside expertees		■										
	total quality management		■				■		■			■	
	internal/external comunication												

Nelle analisi a seguire, gli strumenti sono stati suddivisi oltre che per tipologia "macro" anche per "famiglie"[17] di affinità. Questa suddivisione ha il solo scopo di raggruppare strumenti "simili", ma non vuole approfondire le relazioni che esistono fra tipologie di strumenti differenti. È quindi possibile che coesistano all'interno di una stessa famiglia strumenti di livello atomico con strumenti generici, oppure device tecnologici con politiche gestionali (per esempio nella categoria "macro" sono presenti il TQM e le certificazioni, strumenti radicalmente diversi e non confrontabili). Di seguito viene fornita una descrizione di ogni categoria "macro" e di ogni "famiglia" di classificazione degli strumenti.

3.2.1 Facility management

Tabella 20: Facility management

MACRO	FAMIGLIA	STRUMENTO
FACILITY MANAGEMENT	Warehouse/terminal layout design	guarded gate
		Lighting
		clearly marked control areas
		establish driver waiting areas
		specific equipment for key operational/high-value cargo areas
		minimization of exit/entry point
	Facility protection	Fence
		Locks
		Wall
	Facility monitoring	closed circuit television
		alarm system
		Surveliance
	Access/presence control processes and technologies	acces control system (person and vehicles)
		identification system (person and vehicles)

All'interno di questa categoria rientrano tutti quegli strumenti che *"garantiscono la sicurezza della struttura nella quale i cargo sono immagazzinati e gestiti"* (Gutierrez e Intsa, 2006). Si tratta di strumenti che consentono *"la prima linea difensiva per le intrusioni. In particolare, le strutture di gestione e stoccaggio dei cargo in territorio*

[17] Mentre le categorie "macro" che sono state individuate dalla letteratura, le "famiglie" sono state da noi inserite per organizzare in maniera più strutturata la classificazione. Le famiglie vogliono solo riunire strumenti simili con applicazione nello stesso ambito aziendale

nazionale o estero, devono avere delle barriere fisiche e altri deterrenti che sorveglino rispetto ad accessi non autorizzati" (U.S. Custom and Border Protection, 2006).

Questi strumenti, classificati da Sheffi e Caniato (2003) nell'area della physical security, sono le prime misure di sicurezza che vengono prese in considerazione nella progettazione e realizzazione di un sistema di sicurezza per una struttura logistica. In riferimento alla physical security in generale, Rice e Spayd (2005) affermano che *"questi investimenti possono portare benefici collaterali quali minori costi assicurativi a cusa della minor probabilità di furto e come minori costi indiretti (costi amministrativi di breve termine e spese di lungo termine) che non sono rimborsati dalle polizze assicurative".* Questa categoria è stata suddivisa in quattro famiglie di strumenti.

Warehouse/terminal layout design

Si tratta di strumenti utili in fase di progettazione di una struttura logistica che dovrà gestire e/o stoccare ILU. La famiglia è composta da strumenti come cancelli e ingressi sorvegliati, che hanno l'obiettivo di minimizzare e controllare i punti di ingresso/uscita della struttura. Un'altra tipologia di strumenti sono l'impianto di illuminazione ed il sistema di alimentazione di backup per le aree adibite ad ospitare ILU di alto valore, per assicurare un sistema di difesa attivo 24 ore su 24. Altri strumenti riguardano invece la predisposizione di zone adibite all'attesa di mezzi e autisti all'interno della struttura, e all'individuazione delle zone ad alto rischio per la quale è necessaria una particolare attenzione nella supervisione o sono necessari sistemi fisici per il controllo all'accesso. Harrald et al. (2004) mostrano come per i carichi ad alto valore le strutture per trasferire i container da una modalità all'altra vengano specificatamente disegnate per garantire protezione e controlli maggiori.

Donner e Kruk (2009) affermano che i progetti per la messa in sicurezza dei container devono prevedere *"la ri-configurazione del layout dei terminal portuali in modo da inserirvi le attrezzature necessarie senza compromettere l'efficienza"*.

Facility protection

All'interno di questa categoria rientrano quegli strumenti di difesa fisica delle strutture logistiche adibite alla gestione e stoccaggio di ILU.

Nel dettaglio fanno parte di questa famiglia strumenti come muri, recinzioni e lucchetti.

Facility monitoring

Fanno parte di questa famiglia gli strumenti che consentono un monitoraggio costante della struttura logistica, come i sistemi di telecamere a circuito chiuso o il personale di

sicurezza qualificato adibito alla sorveglianza della struttura, o come i sistemi d'allarme anti-intrusione con dispositivi per la segnalazione di pericoli e anomalie.

Acces/presence control processes and technologies

All'interno di questa famiglia sono presenti i sistemi di controllo all'accesso e d'identificazione sia per persone che per veicoli. Mentre i primi hanno il solo obiettivo di limitare l'ingresso alla struttura (o a zone della struttura logistica) al solo personale e veicoli autorizzati, il secondo sistema ha anche l'obiettivo di identificare e controllare in tempo reale le persone e i veicoli che sono in una determinata zona della struttura. Questo è anche possibile implementando una politica di color coding per le uniformi di lavoro, o con l'utilizzo di badge identificativi che permettono un ingresso selettivo del personale alle diverse zone della struttura.

3.2.2 Cargo management

Rientrano in questa categoria tutti quegli strumenti che *"garantiscono la protezione del cargo durante tutti gli step del processo di trasporto"*.(Gutierrez e Intsa, 2006) Suddividendo ulteriormente questa categoria è stato possibile individuare gli strumenti che si occupano della messa in sicurezza del processo di trasporto (Conveyance management) da quelli più specificatamente utilizzati per la messa in sicurezza delle ILU (ILU management).

3.2.3 Conveyance management

Tabella 21: Conveyance management

MACRO	FAMIGLIA	STRUMENTO
CONVEYANCE MANAGEMENT	Inspection during the shipping process	inspecting conveyance in route and in handling point
	Cargo tracking and identification technical solutions	RFID system
		barcode & scanning cards
		Supply Chain Event Management (SCEM)
		wireless sensor network
		tracing cargo with driver data port
		GPS
	Vehicle anti-tampering solutions	security escorts to and from the port
		vehicle immobilisation device
	Route management	green lanes
		avoid travelling through high-risk areas

avoid parking in high-risk areas
avoid stops en route
route security system

Gli strumenti di Conveyance management assicurano che il processo di trasporto non faciliti un atto terroristico o un sabotaggio/manipolazione intenzionale, e che l'intero trasporto delle ILU sia in grado di sopportare e reagire ad una disruption.
Fanno parte di questa categoria quattro famiglie di strumenti.

Inspection during the shipping process

Fanno parte di questa famiglia tutte le politiche di ispezione e controllo delle ILU nell'intero processo di trasporto, dai punti di origine/destino, ai terminal intermodali fino ai controlli durante il tragitto su strada. Sono politiche necessarie per garantire da un lato la sicurezza del trasporto e dall'altro il controllo, da parte del committente (MTO o cliente industriale), su chi materialmente esegue il trasporto.
Donner e Kruk (2009) spiegano che *"non ci sono studi che stabiliscono chiaramente il maggior impatto sui costi che si otterrebbe con lo screening del 100% dei container comportando una riduzione di efficienza delle operation dei terminal portuali per l'effetto di rallentamenti dei flussi fisici"*. Le tecniche di ispezione verranno approfondite nella famiglia di ILU ispection solutions.

Cargo tracking and identifications technical solutions

In questa famiglia sono presenti gli strumenti che consentono di aumentare la visibilità sull'intero processo di trasporto. Per un'azienda la visibilità sul processo è determinante come evidenziato precedentemente nel paragrafo 2.3.4: infatti, come afferma Sarathy (2006) *"l'aumento di visibilità sulla localizzazione e sullo stato di avanzamento dei container lungo la supply chain e la conoscenza dettagliata del loro contenuto e della data di arrivo, consente benefici in termini di riduzione del livello delle scorte, degli stock-out e di furti e comporta un miglior servizio dell'importatore e migliori relazioni tra i partner"*.
In particolare le tecnologie RFID sono state ampiamente studiate in termini quantitativi (Bearing Point, paragrafo 2.3.4; Motorola, 2004) e qualitativi nella loro relazione con le prestazioni di visibilità e efficienza (Willis e Ortiz, 2004; Daschkovska et al., 2008; Williams et al., 2008). I sistemi RFID consentono un controllo della sicurezza fisica del trasporto e la gestione e trasmissione di dati riguardanti il processo door to door. Le unità di trasmissione dati, i tag RFID, possono essere applicati sia sulla ILU che

direttamente sulla merce trasportata e solitamente sono associati a sigilli elettronici. Esistono diverse tipologie di sensori che possono monitorare differenti parametri del trasporto, a seconda delle esigenze. Come rilevano Willis e Ortiz (2004) la tecnologia RFID *"vuole rendere la supply chain più trasparente, permettendo ai trasportatori di tracciare le spedizioni dal punto di origine fino a destino. Con un network trasparente, i trasportatori possono capire i colli di bottiglia della propria supply chain e possono potenzialmente migliorare la propria efficienza. La trasparenza può ridurre i costi relativi ai furti e ai prodotti smarriti tramite il rilevamento preventivo di errori di instradamento o prodotti non approvati. La rilevazione di inconsistenze nel contenuto dei container, se osservate al porto di origine, riduce sia i potenziali danni terroristici che le frodi. La rilevazione al porto di destino può diminuire le perdite causate da frodi. I sistemi RFID contribuiscono anche ad abbassare le conseguenze di disruption. Pur non modificandone le cause, hanno la capacità di localizzare e reindirizzare rapidamente le spedizioni a seguito di eventi calamitosi, migliorando la resilienza della supply chain".* Secondo Williams et al. (2008), con riferimento all'applicazione di un sistema RFID, *"lo sforzo di sicurezza porta a benefici finanziari, ed includono un aumento della visibilità, l'evitare costi d'importazione, la riduzione delle scorte di sicurezza, l'aumento del servizio al cliente, un miglior profitto e una riduzione dei furti".*

Le scanning cards con barcode sono altri strumenti appartenenti alla famiglia. Devono viaggiare con gli autisti e consentono la trasmissione elettronica di dati riguardanti lo stato del trasporto mediante scansioni ad ogni step del processo. In questo modo è possibile controllare lo stato di avanzamento del trasporto. Facendo un confronto tra tecnologie RFID e barcode, McFarlane e Sheffi (2003) affermano che *"il vantaggio degli RFID risiede nell'efficienza nel processo di carico semplificandolo e eliminando il compiti manuali di lettura del carico e dei pallet; questo sistema è preferibile alla lettura di codici a barra che potrebbero non essere sempre precisi. I risparmi che si ottengono sono quindi in termini di operatività e di accuratezza"*.

I sistemi GPS sono utilizzati dalle aziende per ottenere informazioni real-time sul posizionamento del mezzo e per controllare lo stato di avanzamento del trasporto. Possono essere collegati a sistemi automatici di rilevamento ritardi o anomalie nel tragitto.

I driver data port sono strumentazioni presenti sui mezzi stradali che consentono all'autista di avere un canale di comunicazione diretto con l'azienda; solitamente si

tratta di sistemi GPS integrati con un palmare a disposizione del conducente, che gli permette di scambiare informazioni con l'azienda.

Un passo avanti ulteriore è portato dall'utilizzo di un sistema SCEM (Supply Chain Event Management) che consente mediante un sistema satellitare integrato sui mezzi di trasporto e sulle ILU di trasmettere e gestire informazioni real time sul trasporto, che vanno dallo stato di avanzamento dello stesso, all'integrità del mezzo, alla segnalazione e registrazione di tutte le anomalie che possono avvenire nel processo door to door.

Vehicle anti-tampering solutions

Si tratta di soluzioni per ridurre la probabilità di furti o manomissioni che non sono pensate esclusivamente per la protezione della ILU ma dell'intero vettore.

In particolar modo trattando merce ad alto valore è possibile pensare di scortare il mezzo nei tratti del trasporto più critici (cambio modalità di trasporto o momento di passaggio di responsabilità tra due attori della filiera intermodale o ingresso/uscita da un'area di sosta), o dotare il mezzo di un dispositivo di immobilizzazione dell'intero veicolo (in riferimento ai trattori stradali) che non ne consente l'accensione a meno che non sia il suo autista a metterlo in moto (il meccanismo sfrutta una chiave magnetica che l'autista deve portare con se).

Purtell (2006), attraverso uno studio qualitativo, dimostra che predisporre una scorta lungo il tragitto può portare benefici in termini di costi, nel caso in cuio la merce sia ovviamente di valore e appetibile ai furti.

Route management

Fanno parte di questa famiglia tutti quegli strumenti che hanno l'obiettivo di progettare l'intera rotta che la ILU deve effettuare da origine a destino,

I sistemi più semplici prevedono una pianificazione una tantum delle rotte che tengano conto dei percorsi più sicuri dal punto di vista delle potenziali minacce intenzionali, che consentano di evitare soste intermedie in aree a rischio e parcheggi non custoditi, fino alla creazione di "green lanes", ovvero trasporti effettuati senza nessun tipo di interruzione (per quanto riguarda ispezioni, soste intermedie ed eventuali controlli doganali), abilitate da sigilli elettronici, severi controlli e certificazioni. Un operatore, per ottenere il trattamento "green lane", deve aderire a programmi di certificazione volontaria in ambito security (es C-TPAT, AEO) e dimostrare che tutto il processo sotto la propria area di responsabilità abbia gli adeguati requisiti di sicurezza (includendo i partner di filiera e i subcontractor).

I sistemi più evoluti incorporano queste informazioni in software di "route security system", che riescono a gestire in tempo reale eventuali anomalie riprogrammando di volta in volta il percorso più sicuro.

Nassimbeni (2009), a proposito di pratiche gestionali che ostacolano la ripetitività, afferma che *"tutte le variazioni rispetto alla routine, ad esempio […] la rotta dei trasporti, ostacolano possibili disruption"*. Al contrario, percorsi prestabiliti e ripetitivi aumentano la vulnerabilità ma permettono invece *"l'accumulazione di esperienza sui percorsi tradizionali* (che) *favorisce le economie di scala, con un guadagno di efficienza".*

Le "green lanes", al contrario degli altri strumenti, non presentano alcun trade-off tra le prestazioni di sicurezza e efficienza, ma comportano addirittura un aumento di efficienza attraverso minori ispezioni e soste intermedie. In riferimento alle green lanes Daschkovska et al. (2008) affermano che *"oltre ad ottenere minori ritardi alla dogana, l'implementazione di un alto livello di sicurezza nel processo di trasporto di container produce effetti positivi sull'efficienza dell'intero processo, come la riduzione di costi logistici, delle scorte e l'aumento del livello di servizio.*

3.2.4 ILU management

Tabella 22: ILU management

MACRO	FAMIGLIA	STRUMENTO
ILU MANAGEMENT	ILU inspection solutions	visual ispection/screening
		remote screening/portal sensors
		metal detection
		x-ray checking
		weighted product
		Mirror
	ILU anti-tampering solutions	anti-tamper seals
		e-seals
		smart box
		RFID system
		holistic approach to seal
		global seal control
		plastic seals to secure empty containers
		assigning parking space
		managing container inventory
		limit cargo hold time
		specialized packaging

Gli strumenti di ILU management si focalizzano esclusivamente sulla sicurezza della ILU in relazione a potenziali minacce intenzionali. Fanno parte di questa categoria due famiglie di strumenti.

ILU inspection solutions

Fanno parte di questa famiglie tutte le tecniche e le tecnologie di ispezione delle ILU. Una delle tecniche più utilizzate è la "7-point inspection" che comprende la verifica della parete frontale della ILU, della parete destra, sinistra del fondo e del tetto, dei portelloni interni/esterni e delle pareti esterne del contenitore.

Le tecniche più semplici consistono nell'ispezione a vista che comprende la verifica dell'integrità dei sigilli ed eventualmente la verifica dello stato della merce trasportata e della completezza del carico, sfruttando specchi per la verifica del fondo della ILU.

Ispezioni ulteriori possono consistere nella verifica del peso della merce trasportata per controllare eventuali anomalie.

Tecniche più evolute consentono lo screening da remoto delle ILU sfruttando tecnologie che utilizzano raggi-x o rilevazione di metalli, utili per evitare che il contenitore possa essere utilizzato come un'arma per un potenziale attacco terroristico. Come rilevano Willis e Ortiz (2004) è evidente che tutte le tecniche d'ispezione portano con sé un trade-off tra aumento della sicurezza e diminuzione dell'efficienza. Infatti *"incrementare le ispezioni può aumentare la sicurezza ma incrementa anche le attese e i ritardi nel trasporto. Le decisioni sulla progettazione e gli investimenti in politiche e tecnologie di sicurezza deve sempre valutare i trade-off esistenti tra le cinque prestazioni chiave della supply chain (efficienza, resilienza, tolleranza alle anomalie, trasparenza e affidabilità del trasporto), e considerare la loro importanza relativa nel contesto di una decisione specifica".[…] Spesso la loro applicazione è stata limitata per i costi delle attrezzature, la mancanza di spazio nei terminal portuali, il tempo richiesto alle operazioni di scanning e il tasso relativamente alto di falsi-positivi derivanti dalle imprecisioni della tecnologia".* In riferimento alla resilienza essi affermano che *"lo scanning dei container non aiuta a ridurre le conseguenze perché non pone rimedio agli effetti di un attacco terroristico".*

Nonostante recenti progetti pilota mostrano che le tecnologie più avanzate d'ispezione delle ILU siano tecnicamente fattibili, ciò che ne ostacola la diffusione sono principalmente questioni di costo, tempo, responsabilità, istruzione/formazione e mancanza di integrazione (IMCOSEC, 2010).

ILU anti-tampering solutions

Costituiscono questa famiglia tutti gli strumenti che vogliono evitare la manomissione delle ILU.

Gli strumenti più semplici sono costituiti dai sigilli meccanici. Questi vengono applicati sul portellone e sono progettati per evidenziare manomissioni o intrusioni della ILU e per assicurare la chiusura delle porte del contenitore. Ogni sigillo è contrassegnato da un codice identificativo (ed eventualmente da un logo che individua il trasportatore) associato in maniera univoca ad ogni trasporto, così che in caso di intrusione nella ILU e sostituzione del sigillo durante il trasporto sia possibile rilevare l'anomalia in fase di controllo in ingresso del cargo. Esistono varie tipologie di sigilli meccanici che vanno dai padlock seal, ai cable seal, ai bolt seal, ai barrier seal, ai security seal fino agli indicative seal a seconda del tipo di ILU e della tipologia di trasporto (dettagli in Appendice A). I sigilli di plastica vengono invece utilizzati per assicurare i container vuoti.

"I sigilli anti-manomissione incrementano le capacità d'individuazione anomalie ai terminali di origine e arrivo. L'individuazione al terminale di partenza riduce i potenziali danni da azioni terroristiche o fraudolente. L'individuazione al terminale di arrivo riduce esclusivamente i danni potenziali derivanti da azioni fraudolente. […] I sigilli anti-manomissione non hanno un impatto significativo sull'incremento dell'efficienza della supply chain. Le riduzioni di tempo nelle ispezioni e nel tempo di processamento sono modesti e vanno a compensare il costo d'investimento per l'acquisizione degli stessi dispositivi di sicurezza. I sigilli anti-manomissione, inoltre, non aiutano nella mitigazione degli effetti quando si verifica una disruption" (Willis e Ortiz, 2004).

Il processo completo di verifica e gestione dei sigilli, definito dall'U.S. Custom and Border Protection (2006) *"approccio olistico"* è così strutturato: il numero del sigillo viene trasmesso elettronicamente dal trasportatore al partner successivo di filiera (che può essere il cliente finale o intermedio) prima dell'arrivo della ILU a destino. All'arrivo del mezzo chi è responsabile del controllo dei sigilli, con l'aiuto dell'autista, verifica sia l'integrità del sigillo sia la corrispondenza del codice del sigillo con la bolla di carico. Prima di lasciare definitivamente il carico, l'autista deve trasmettere l'avvenuto rilascio della ILU alla propria azienda, così che possa essere elettronicamente verificato il passaggio di responsabilità senza intoppi. Per la procedura

d'uscita, infine, l'autista dovrà poi passare l'ultima barriera di controllo del cliente finale o intermedio.

Per far si che il processo sia totalmente sicuro, è inoltre necessario un approccio definito dall'U.S. Custom and Border Protection (2006) *"global seal control"* il quale prevede che l'approccio olistico sia applicato da tutti i partner e fornitori terzi di servizio all'interno della supply chain, per garantire integrità e sicurezza nell'intera catena. Inoltre il numero del sigillo deve essere trasmesso con codifiche elettroniche protette in tutti gli handling point della filiera.

Una tecnologia più evoluta di sigilli è costituita dai sigilli elettronici (e-seals) che hanno lo stesso principio di funzionamento di quelli meccanici, ma oltre a controllare l'integrità fisica della ILU hanno capacità di raccogliere, immagazzinare e trasmettere informazioni aggiuntive. Le informazioni possono riguardare il contenuto della ILU, lo stato del traporto e il luogo e tempo di possibili attacchi all'integrità del cargo (smart box). Solitamente questi sigilli sono collegati a vari sensori che possono monitorare differenti aspetti dell'evoluzione del traporto. Le tecnologie più diffuse di trasmissione dati si possono raggiungere utilizzando RFID e infrarossi.

Secondo Daschkovska et al., 2008; Donner e Kruk, 2009, attraverso l'implementazione di tutti i tipi di e-seals è possibile migliorare congiuntamente sicurezza e efficienza del processo di trasporto dei container lungo l'intera supply chain attraverso: *"l'aumento dell'efficienza si può potenzialmente riscontrare attraverso la riduzione dei lead time nel processo di ispezione. […] Un e-seal è in grado di contenere informazioni, mantenere la visibilità in rotta e permettere la segnalazione di eventi in real time"* (Daschkovska et al., 2008).

"Gli e-seals hanno chiaramente numerosi vantaggi rispetto ai sigilli meccanici. Possono essere usati per identificare container e segnalare intrusioni automaticamente, cosa che i dispositivi meccanici non possono fare. Inoltre gli e-seals possono essere collegati a sensori per la rilevazione di movimento, intrusioni su ognuno dei sei lati del container, pericoli radioattivi, biologici o chimici. Non è però ancora disponibile uno standard internazionale per i sigilli elettronici, per la presenza di differenti problematiche: in prima istanza non esistono frequenze uniformi tra differenti paesi, adottate per la trasmissione dati. […] Secondo, l'integrazione tra i prodotti di vendor diversi non è assicurata. Infine, la maggior parte dei terminali e strutture logistiche dove i container sono manipolati non trovano valide giustificazioni finanziarie per

investire in strumenti e infrastrutture di lettera automatizzata. Il risultato è che nessun sigillo elettronico può essere utilizzato a livello internazionale". (Downey, 2006)

Tutti i sistemi di questo tipo che utilizzano sigilli di garanzia, non offrono informazioni dirette sullo stato della merce trasportata, ma offrono informazioni sullo stato del sigillo; è quindi è possibile che l'integrità della ILU possa essere compromessa senza la compromissione del sigillo (per esempio smontando un'intera parete della ILU il sigillo risulta integro anche se è stato possibile compromettere la merce).

Oltre a queste tecnologie è importante eseguire un'appropriata gestione delle ILU, per esempio con un sistema barcode che consenta di individuare tutte le ILU stoccate in un deposito/piazzale, e limitare possibili fonti di rischio interno nelle strutture ricettive, come limitare il tempo di sosta massima di un cargo o assegnare precise aree di parcheggio per i vettori stradali. In più un packaging diversificato (es. con diversi colori a seconda della merce o del trasportatore) può aiutare nel controllo visivo su piazzale.

3.2.5 Information management system

Tabella 23: Information management

MACRO	FAMIGLIA	STRUMENTO
INFORMATION MANAGEMENT	Quality information/data	complete and accurate information
		integration of data from different sources
		automated information (B2Custom --> ACE; B2B --> EDI)
		secure elettronic data transmissions
		reporting irregularities
		advance information (B2C -->ATDI; B2B --> ASN)
	Protection of business information/data	destroy sensitive documents
		safeguard computer access
	Recordkeeping of information	back up data
		record personnel information
		record knowledge of workers

Rientrano in questa categoria gli strumenti che *"proteggono i dati critici del business e utilizzano le informazioni come mezzo per individuare anomalie e prevenire lacune di sicurezza"* (Gutierrez e Hintsa, 2006).

Costituiscono questa categoria tre famiglie di strumenti.

Quality information/data

Fanno parte di questa famiglia gli strumenti che consentono all'azienda di poter gestire un database informativo di qualità. Per informazioni s'intende sia quelle riguardanti il normale business, con impatti sull'operatività quotidiana, sia quelle riguardanti eventi specifici, come anomalie, incongruenze, attacchi. Gli autori van Oosterhout et al. (2006), hanno individuato nove blocchi informativi principali che devono essere conosciuti per poter gestire il processo di trasporto in sicurezza.

Il primo riguarda le "booking information" relative a codici identificativi e informazioni sulle prenotazioni delle linee di traffico. Il secondo comprende le "cargo information" che contengono informazioni sulla merce trasportata dalle ILU e sullo stato di avanzamento del cargo nel processo di trasporto. Il terzo e quarto gruppo contengono le informazioni derivanti dalle ispezioni effettuate con diversi tipi di tecnologie come raggi-X e physical ispection, o metal detection. Il quinto gruppo fornisce le informazioni sul "container (status)" che riguardano il numero della ILU, il proprietario della ILU e lo stato dei sigilli. Il sesto gruppo, "operator & location information" contiene informazioni sui luoghi di manipolazione del container, come i terminal di origine e destino e i luoghi di carico/scarico, e degli operatori che hanno preso in consegna il contenitore (nomi e se sono certificati o meno). Il settimo gruppo riguarda le "seal information", quali tipologia di sigillo, numero identificativo, luogo di chiusura del sigillo e tutte le informazioni riguardo a eventuali compromissioni dell'integrità del sigillo. L'ottavo gruppo comprende le "certificate information" che riguarda la tipologia di certificazione che possiedono le compagnie di trasporto, la durata e la validità. Il nono gruppo riguarda invece le "personnel information" che comprende tutte le informazioni sul personale che è entrato in contatto con le ILU durante il processo di trasporto.

Le tecnologie elettroniche aiutano ad ottenere un database informativo di qualità, riducendo incomprensioni ed errori umani. D'altro canto risultano più critici gli aspetti d'integrazione dati da differenti fonti informative (dove non esiste uno standard di codifica delle informazioni) e di protezione del canale di trasmissione delle informazioni, per evitare il rischio di accesso illegittimo ad informazioni sensibili.

La comunicazione elettronica consente anche di trasmettere anticipatamente informazioni critiche, per velocizzare le operazioni di controllo e ispezione e aiutare nella progettazione efficiente e sicura della supply chain.

Per l'automazione e la facilità di trasmissione dati è importante riferirsi a standard di comunicazione sia B2B che B2C, come sistemi EDI (elettronic data interchange) utili per scambiarsi informazioni ad alto contenuto qualitativo. *"L'introduzione di strumenti di automated data collection nelle container supply chain ha abilitato un collegamento più veloce rispetto al passato tra gli attori della filiera del trasporto, mentre ha ridotto il bisogno di formazione degli utilizzatori su processi per la raccolta dei dati e minimizzato la necessita di integrare i dati provenienti da sistemi proprietari di tipo legacy. [..] Il risultante guadagno in termine di efficienza è stato stimato in un risparmio di 5-7 miliardi di dollari all'anno"* (Motorola, 2004).

Per la gestione delle anomalie è invece importante riportare in modo standard e formale tutte le irregolarità verificatesi nell'operatività quotidiana, per costruire una base di dati valida per il supporto alle decisioni.

Lo strumento di Advanced Data *"aiuta le organizzazioni e le autorità governative a comunicare anomalie e discrepanze prima dell'arrivo del carico. Oltretutto, consente di trasmettere anticipatamente informazioni critiche per velocizzare le operazioni di controllo e ispezione e di aiutare nella progettazione efficiente e sicura della supply chain* (U.S. Custom and Border Protection, 2006).

Protection of business information/data

Si tratta di procedure più pratiche per la protezione delle informazioni in azienda come l'archiviazione dei dati in luoghi sicuri o la distruzione di documenti che contengono informazioni critiche, piuttosto che la protezione con accessi selettivi a determinate aree dell'azienda e password per l'autenticazione all'accesso mediante computer. Nassimbeni (2009) afferma che variazioni di routine come il cambio di password per assicurare la protezione delle informazioni diminuiscono il rischio di spillover delle informazioni riservate, ma diminuiscono anche l'efficienza.

Recordkeeping of information

Si tratta degli strumenti che consentono di memorizzare e archiviare informazioni relative al personale d'azienda, di gestire la conoscenza mediante codificazione dell'esperienza e di creare database di backup ai quali possono accedere solo determinate figure all'interno dell'azienda. L'obiettivo di questi strumenti è quello di aiutare l'azienda a gestire e superare qualsiasi tipo di disruption.

3.2.6 Business network & company management system

Tabella 24: Business network & company management system

MACRO	FAMIGLIA	STRUMENTO
BUSINESS NETWORK & COMPANY MANAGEMENT SYSTEM	company security management system	laws and certifications (ISO, AEO)
		std procedure
		risk management
		emergency plan (Business Continuity Planning, Crisis Management)
		inventory management system (SS/ emergency stock)
		monitor and synthesize information regarding security practise
		alert system
		Security function/position (CSO)
	logistic system design	total quality management
		additional capacity
		reconfigurable resource and planning
		reconfigurable product
		reconfigurable SC network
		Postponement
	business partner evaluation system	audits of partners' system security
		certifications (AEO, third-tier status)
	collaborative relationship with partner and administration	supplier base selection and reduction
		integrated SC management
		external comunication (feedback on requirements and performances)
		inform government regarding known vulnerabilities
		involves partners in setting security standards
		sharing responsabilità

Rientrano in questa categoria gli strumenti che sono necessari per *"costruire una struttura organizzativa interna ed esterna sicura, ed un sistema di gestione aziendale di qualità".* (Gutierrez e Hintsa, 2006)

Questi strumenti non sono pensati con specifico focus sulla sicurezza ma i loro impatti sono importanti anche sotto questo aspetto. Costituiscono la categoria quattro famiglie di strumenti.

Company security management system

Fanno parte di questa famiglia quegli strumenti che riguardano la progettazione e l'implementazione di un sistema di gestione della sicurezza (security). Rice e Spayd (2005) affermano che *"un sistema di gestione della sicurezza deve essere disegnato in modo da migliorare la sicurezza senza aumentare i costi e la complessità della supply chain"*.

In prima istanza riguardano l'istituzione in azienda di una funzione o una figura con specifica competenza sulla security (il chief security officer CSO); il suo compito è quello di controllo e aggiornamento continuo delle procedure, oltre alla comunicazione e diffusione delle procedure di sicurezza a tutti i livelli aziendali. Urciuoli (2009) afferma che *"è fondamentale formare e educare figure professionali capaci di integrare e armonizzare soluzioni di sicurezza nella supply chain senza compromettere l'efficienza. Questa integrazione deve essere perseguita dall'educazione dei manager della logistica e della supply chain sulle aree di sicurezza da considerare in attività di risk management e di valutazione del rischio"*.

La standardizzazione delle procedure di sicurezza e il loro monitoraggio sono il punto di partenza per l'implementazione di un buon sistema di sicurezza. Inoltre, *"adottando standard per la sicurezza, il coordinamento e le operation, le aziende possono aumentare l'efficienza dei processi logistici e ridurre potenzialmente i tempi di trasporto"* (Rece e Spayd, 2005)

Per quanto riguarda il lato più operativo, le procedure di gestione delle scorte (scorte di sicurezza e scorte di emergenza) e i piani d'emergenza (crisis management, business continuity planning) consentono all'azienda di aumentare la propria resilienza.

I sistemi più evoluti, con l'ausilio di software appositi di allerta, permettono il controllo real time del processo, con la possibilità di intervenire in maniera tempestiva in caso di segnalazione di un'anomalia.

Tutte queste iniziative per essere efficaci, devono essere coerenti con un programma di risk management che stabilisca obiettivi, politiche ad alto livello e controlli periodici sullo stato del sistema di gestione della sicurezza. Un programma di risk management favorisce *"lo sviluppo di procedure e politiche scritte per il reporting, la documentazione e l'analisi di incidenti, tali da assicurare un sistema efficiente ed efficace"* (U.S. Custom and Border Protection, 2006)

Una volta progettato e implementato un sistema di gestione della sicurezza, le certificazioni effettuate da un ente esterno all'azienda sono uno strumento efficace per

verificare la qualità del sistema, con impatti anche sul business quotidiano. Infatti le certificazioni che attestano l'aderenza alle best security practice possono corrispondere a minori ispezioni e soste intermedie durante il trasporto, e quindi la possibilità di progettare una supply chain più efficiente e sicura.

In questo processo di diffusione di standard best practice e di certificazioni volontarie che attestino l'aderenza a queste pratiche, promosso dal WCO, si è sviluppato in Europa il concetto di AEO. Come spiegato da Urcioli (2009) *"l'obiettivo finale degli standard è facilitare il commercio globale. Lo scopo dell'iniziativa AEO è di rilevare i cargo ad alto rischio il prima possibile nella supply chain, in un modo efficiente e poco dispendioso dal punto di vista delle risorse utilizzate. Per ottenere la certificazione, le aziende devono essere conformi ad un preciso set di criteri come: conformità storica ai controlli doganali, adozione di un appropriato sistema di documentazione e reporting commerciale, solvibilità finanziaria, scambi informativi, misure di sicurezza nel trasporto, monitoraggio del cargo e del personale e seguire le linee guida relative all'integrità e consistenza del sistema di sicurezza. Così facendo, ogni barriera doganale europea è stimolata a creare partnership con il settore privato e classificare il loro sistema di sicurezza. L'iniziativa AEO si crede possa portare ad una situazione win-win tra aziende e controlli doganali. Le compagnie aderenti alla certificazione beneficeranno di procedure più rapide di ispezione, mentre la dogana potrà migliorare l'utilizzo efficiente delle proprie risorse"*.

Logistic system design

Questa famiglia comprende strumenti che in fase di progettazione di un sistema logistico gli garantiscono flessibilità, così da poter reagire ad eventuali disruption con tempi e costi contenuti.

Gli strumenti si riferiscono alla possibilità di avere un network della supply chain facilmente riconfigurabile, per esempio potendo disporre di più modalità di trasporto o non essendo vincolati a strutture e partner logistici, o avendo flessibilità nei contratti di fornitura. La riconfigurabilità può riguardare anche le risorse a disposizione dell'azienda (dalle macchine alle risorse umane) e la possibilità di effettuare una programmazione delle attività senza particolari colli di bottiglia o vincoli.

Come rileva Nassimbeni (2009) *"la flessibilità di un sistema perturbato dipende non soltanto dalla sua componente hardware, bensì anche dalle modalità soft di gestione*

del flusso: programmazione e controllo della produzione, gestione delle scorte, criteri di allocazione delle risorse".

Un ulteriore strumento a sostegno di una supply chain flessibile è l'implementazione di una strategia di postponement. "*Modifiche nella progettazione dei componenti, che intervengono ad esempio sul loro numero, sul loro livello di standardizzazione, sulle comunanze esistenti tra prodotti, insieme ad un design for manufacturing, for assembly e for agility finalizzato alla semplificazione dei processi e al posticipo delle scelte di configurazione definitive, possono ridurre sensibilmente le vulnerabilità"* (Nassimbeni, 2009).

Queste politiche rientrano in una strategia ad alto livello, che si rifà ai principi del Total Quality Management. I programmi di TQM consentono di *"disegnare dei miglioramenti che aumentano l'affidabilità della filiera e allo stesso tempo la riduzione dei costi e aumento di produttività"* (Burmeisters e Solovjovs, 2009). Lee e Wolf (2003), Lee e Whang (2005) e Rice e Spayd (2005) affermano che i principi del TQM possono condurre contemporaneamente a un maggior livello di sicurezza, efficienza, efficacia e profittabilità. Inoltre, Rice e Spayd (2005) affermano che il TQM possa avere anche un impatto sulla maggior visibilità dei colli di bottiglia della filiera.

Con il medesimo obiettivo degli strumenti sopracitati di ottenere flessibilità e migliorare la resilienza, l'altra strategia è quella di cautelarsi con della capacità addizionale; in tutti e due i casi sono presenti trade-off tra costi e benefici (Nassimbeni, 2009) e la via preferibile da seguire varia in base al contesto.

Come rileva Sheffi (2005) *"la resilienza può essere raggiunta tramite ridondanza o flessibilità. Gli utilizzi standard della ridondanza riguardano scorte di sicurezza di materiali o prodotto finito. Tali scorte possono dare ad un'azienda il tempo per pianificare la sua strategia di recupero. […] Le scorte addizionali, però, sono costose da mantenere. Inoltre, come dimostrato dai processi lean e six sigma, possono portare a operation inefficienti, con risultato conseguente di costi addizionali e qualità inferiore. Per contro, un aumento della flessibilità della supply chain può aiutare un'azienda non solo ad affrontare una disruption ma anche a rispondere in maniera migliore ai capricci giornalieri del mercato"*.

Business partner evaluation system

Questa famiglia comprende gli strumenti che garantiscono ad un'azienda che i propri fornitori e subcontractor assicurino la stessa qualità e sicurezza dell'azienda stessa. È

evidente che essendo il trasporto intermodale composto da diverse tipologie di attori e da vari passaggi di responsabilità, l'inadeguatezza di un player determina una cattiva prestazione dell'intera filiera. Gli strumenti per ovviare a questo problema sono di due tipi: il primo non prevede un coinvolgimento diretto dell'azienda nella valutazione del partner, ma la scelta di affidarsi ad operatori che possiedano le medesime certificazioni dell'azienda. Il secondo tipo consiste nell'organizzazione di un processo di controllo e valutazione del sistema di sicurezza dei fornitori che possa garantirne la modalità di lavoro. In riferimento alle certificazioni, abbiamo già visto per la famiglia di strumenti di Company security management system come esse comportino vantaggi di efficienza.

Collaborative relationship with partner and administration

In questa famiglia rientrano tutti gli strumenti necessari per stabilire delle relazioni di collaborazione con i partner nella filiera, e con amministrazioni e autorità di riferimento per il territorio.

Avere relazioni collaborative con i player della filiera è fondamentale considerando la pluralità e le diverse responsabilità degli attori coinvolti.

Un processo di selezione e riduzione della base di fornitori è il primo passo che va nella direzione di rafforzare il rapporto di collaborazione con i partner: una base ristretta consente una relazione più forte e integrata, che va nella direzione di una condivisione di rischi e responsabilità, e con l'obiettivo ultimo di una crescita condivisa. Tuttavia, è importante prestare bene attenzione nelle politiche di riduzione della base fornitori, in quanto secondo Jüttner et al (2003) e Nassimbeni (2009) una base troppo ridotta potrebbe anche diventare la fonte di vulnerabilità.

L'approccio strategico aziendale alla sicurezza deve essere influenzato anche dalle caratteristiche dei partner, per esempio nello stabilire gli standard di sicurezza minimi, e molta più attenzione deve essere posta nella comunicazione con il partner, direttamente coinvolto nel processo di miglioramento continuo in ottica di filiera.

Il fine ultimo di una relazione di collaborazione continuativa è quello di poter implementare un sistema di gestione della supply chain integrato nella filiera, che garantisca massima visibilità e trasparenza su tutti i partner, per poter ottenere benefici in termini di sicurezza, efficienza e resilienza.

Tuttavia Nassimbeni (2009), individua un trade-off tra collaborazione con i partner e segretezza e quindi tra efficienza e sicurezza: *"la collaborazione operativa e la condivisione di informazioni sono necessarie per la realizzazione di filiere integrate,*

con vantaggi di reattività ed efficienza del flusso. Ma la condivisione di dati, conoscenze tecnologiche e modalità operative incrementa il rischio di intercettazione di informazioni riservate, di distorsione di informazioni, di comportamento opportunistico di soggetti interni o esterni alla filiera".

Un altro aspetto riguarda il rapporto dell'azienda con le autorità territoriali di riferimento; stabilire un buon rapporto di comunicazione è infatti importante per superare le vulnerabilità della filiera, soprattutto in riferimento alle infrastrutture di trasporto, e poter proteggere gli asset e il business aziendale.

"Le amministrazioni sono responsabili di facilitare gli spostamenti di persone e beni oltre confine e sono responsabili ultimi della sicurezza delle persone, del paese e del commercio. Per le autorità e le agenzie governative, il focus tradizionale è stato il controllo del commercio, per assicurarsi l'introito di tasse, limitando il traffico di merce illegale con ispezioni e controlli sui prodotti in ingresso. Il focus attuale, invece, si sta spostando verso l'agevolazione del commercio con controlli di sicurezza concentrati nelle prime fasi della catena e con l'identificazione di partner fidati che possano aiutare ad incrementare la sicurezza nelle ispezioni sull'export e informazioni durante il trasporto. Il reale significato di partner fidato, però, crea l'esigenza per una cooperazione globale" (Closs e McGarrel, 2004).

L'integrazione delle organizzazioni deve quindi svilupparsi anche in direzione delle autorità governative, con le quali è possibile massimizzare sicurezza ed efficienza nelle operation della supply chain (Sheffi, 2001). "*Le autorità devono continuamente rivedere e aggiornare le procedure di sicurezza con l'obiettivo di migliorare entrambi gli obiettivi di efficienza e sicurezza"* (Closs e McGarrell, 2004). In questo contesto collaborativo, lo sviluppo di standard di sicurezza migliorano entrambe la sicurezza e l'efficienza. (Williams et al., 2008).

3.2.7 Human resource management

Tabella 25: Human resource management

MACRO	FAMIGLIA	STRUMENTO
HUMAN RESOURCE MANAGEMENT	employee hiring and screening process	background investigation on potential employees and third-party providers
		interview/psychological examinations
		hire security-specific skills

employe exit process	employee termination procedure
organizational roles and responsibilities	assign security responsabilities to personnel
	rotating shipping/receiving personnel
	multi-skilled workforce
	estabilish security goals
	measurement system of employee
	incentive system for security

In questa categoria rientrano quegli strumento che *"garantiscono l'affidabilità di tutto il personale in contatto diretto e indiretto con il cargo e con gli asset di altre società"* (Gutierrez e Hintsa, 2006). La categoria è composta da tre famiglie di strumenti.

Employee hiring and screening process

Fanno parte di questa famiglia gli strumenti di ricerca e selezione del personale. In fase di selezione è infatti importante verificare il background di un potenziale dipendente, in particolar modo per i collaboratori occasionali o i dipendenti di enti terzi e, in alcuni casi, è auspicabile allargare la verifica fino ai fornitori. Lo screening deve riguardare la presa visione della fedina penale[18] e delle referenze derivanti da lavori precedenti, oltre che di un colloquio/test per la verifica della propensione alla corruzione dell'individuo. *"Scarse politiche di sicurezza in fase di assunzione possono far conseguire buchi di sicurezza, perdite finanziare significative e diminuzione della produttività. Tutti i buchi di sicurezza hanno una causa in comune… le persone"* (U.S. Custom and Border Protection, 2006). Un altro parametro da considerare in fase di assunzione è la ricerca di personale che abbia maturato specifiche competenze in ambito sicurezza, derivanti da corsi di formazione specializzati o esperienze lavorative precedenti.

Employee exit process

La procedura di fine rapporto per un dipendente deve essere standard e formalizzata dall'azienda; l'utilizzo di checklist può aiutare nell'implementazione della procedura. Lo scopo è quello di evitare di concedere all'ex dipendente la libertà di frequentare aree private aziendali come se facesse ancora parte dell'azienda.

[18] A seconda della legislazione sulla privacy di ogni paese è possibile spingersi più o meno a fondo nella ricerca di informazioni riguardanti il potenziale dipendente

Organizational roles and responsibilities

Fanno parte di questa famiglia gli strumenti necessari per l'organizzazione della struttura organizzativa interna della sicurezza.

Assegnare al personale specifiche responsabilità di sicurezza è il primo passo per l'implementazione di una precisa politica in ambito security che può comprendere la definizione periodica di obiettivi di sicurezza per il personale e un sistema di controllo e misurazione finalizzato a determinare un'incentivazione di tipo economica o non. Ovviamente questa politica, soprattutto se prevede incentivi di tipo economico, deve essere standard e formalizzata per non creare tensioni interne tra il personale.

Importante è anche progettare una forza lavoro con competenze multidisciplinari, così che sia possibile gestire una più ampia gamma di situazioni impreviste, sia nello svolgimento del normale business quotidiano che nella gestione di disruption. Inoltre, come misura preventiva, ruotare il personale adibito alla ricezione e controllo può abbassare la probabilità dello sviluppo di azioni collusive.

3.2.8 Awarness management

Tabella 26: Awarness management

MACRO	FAMIGLIA	STRUMENTO
AWARNESS MANAGEMENT	awareness of procedures adopted by business partner	information dissemination process
		contract with specific security requirements
	Personnel education and training	simulations and excercises
		formal training
		informal socialization
	Security awarness development	security function/position (leadership)
		involve outside expertees
		total quality management
		internal/external comunication

In questa categoria rientrano gli strumento che *"garantiscono la consapevolezza della sicurezza di tutto il personale in contatto diretto e indiretto con il cargo e con gli asset di altre società"*.(Gutierrez e Hintsa, 2006)

La categoria è composta da strumenti di tipo soft e di sviluppo della cultura della sicurezza, ed è formata da tre famiglie di strumenti.

Awarness of procedures adopted by business partner

In questa famiglia sono presenti strumenti che consentono all'azienda di integrare le proprie politiche di sicurezza con quelle del partner, per ottenere una sicurezza totale lungo la filiera. Il riferimento può essere sia al lato operativo, rispetto alle politiche e alle metodologie di lavoro tra le due aziende, ma anche ad un livello più alto con riferimento alla cultura della sicurezza e all'organizzazione del lavoro. A livello pratico alcuni strumenti per raggiungere questo obiettivo sono la raccolta di informazioni lungo l'intero processo di trasporto, per capire le metodologie di lavoro del partner e poter progettare un processo di integrazione, o la definizione di contratti con specifiche clausole sulle metodologie di lavoro e sistemi di controllo della qualità, che il partner deve adottare in ambito security per ottenere piena visibilità/integrazione lungo la filiera.

Personnel education and training

In questa famiglia sono presenti gli strumenti che consentono la formazione continua dei dipendenti in ambito security. Le sedute formative possono essere strutturate con esercitazioni pratiche e simulazioni sul campo, o a livello più teorico con sedute di formazione teorica utilizzando slide o video. Eventi di questo tipo sono momenti d'incontro tra i responsabili della sicurezza in azienda e i livelli più operativi, e sono utili per lo sviluppo del dialogo e della collaborazione tra le parti.

Una politica di questo genere, per essere efficace, deve prevedere riunioni periodiche e un controllo delle prestazioni continuativo che consenta un processo di miglioramento continuo a partire dai punti deboli dell'azienda.

Security awareness development

Questa famiglia comprende tutti gli strumenti che consentono una diffusione in azienda dei principi legati alla sicurezza e un successivo sviluppo della consapevolezza delle tematiche di sicurezza.

La comunicazione è per questo scopo fondamentale sia a livello intra-aziendale, che verso tutti gli stakeholder della supply chain. La figura o la funzione responsabile della diffusione delle tematiche di sicurezza, è indispensabile che abbia caratteristiche di leadership ed abbia il pieno supporto dal lato manageriale, per poter influenzare anche tutti gli altri stakeholder d'azienda. Il coinvolgimento di esperti esterni è una strategia per dimostrare ai dipendenti l'importanza di queste tematiche. In questo senso, Rice e Spayd (2005) evidenziano come la parte più importante dello sforzo di messa in

sicurezza della supply chain riguarda la "socializing security": vuol dire creare e sviluppare il senso di sicurezza della supply chain tra i dipendenti. I principali fattori che interessano la "socializing security" sono la struttura organizzativa d'azienda, la leadership, le competenze maturate dai dipendenti, la formazione dei dipendenti su tematiche di sicurezza, e l'addestramento. Una struttura organizzativa che abbia sviluppato una consapevolezza della sicurezza può *"migliorare la prevenzione di problematiche tramite il riconoscimento anticipato di potenziali problemi da parte di dipendenti […] e può abilitare l'azienda all'intervenire tempestivamente per ridurre l'impatto delle conseguenze di una disruption".* Sempre Rice e Spayd affermano però, che lo sforzo nella "socializing security" può anche portare ad un danno potenziale derivante dallo sviluppo di un falso senso di sicurezza. Questa tesi è supportata anche da Quinn (2003) che sostiene che quando vengono implementati degli sforzi per la sicurezza della supply chain, se questi non sono direttamente ricollegabili a performance aziendali, possono portare allo stallo o all'abbandono nell'implementazione dei programmi. Il risultato è che lo sviluppo e il mantenimento di una cultura aziendale che sostenga l'importanza della sicurezza è critica per la supply chain security. L'insieme di tutte queste iniziative deve essere coerente con una strategia ad alto livello di total quality management, intesa rispetto alle sue implicazioni filosofiche e culturali.

3.3 Analisi degli strumenti

Partendo dagli strumenti di sicurezza individuati, abbiamo deciso di valutare la densità delle macrofamiglie di strumenti (numero di citazioni della macrofamiglia di strumenti sul totale di citazioni possibili della stessa all'interno di tutti gli articoli, in riferimento alla Tabella 27 e Tabella 28 corrisponde al quoziente tra le caselle grigie e il totale delle caselle di una singola macrofamiglia) e riassumere le loro relazioni con le prestazioni organizzative, con lo scopo di identificare eventuali tematiche poco sviluppate.

3.3.1 Analisi della densità

Per ricavare la densità degli strumenti citati negli articoli, abbiamo calcolato la percentuale di citazioni per ogni categoria "macro". Lo scopo è di ottenere un loro confronto per capire quali sono le meno trattate dagli autori considerati nella nostra analisi della letteratura. A partire dalle tabelle di pag. 64-71 abbiamo aggregato i dati

rispetto alla dimensione famiglia, segnalando in Tabella 27 e Tabella 28 quando l'articolo parla almeno di uno degli strumenti appartenenti alla famiglia e il calcolo della densità per ciascuna macro famiglia.

Tabella 27: Calcolo della densità per Facility Management, Cargo Management e Information Management

MACRO	FAMIGLIA	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)	(18)	(19)	(20)	(21)	(22)	(23)	(24)	(25)
FACILITY MANAGEMENT	Warehouse/terminal layout design		■	■	■			■	■						■	■	■					■	■		■	
	Facility protection		■	■	■			■	■						■	■	■	■				■	■		■	
	Facility monitoring		■	■	■		■	■	■						■	■	■	■				■	■		■	
	Access/presence control processes and technologies		■	■	■		■	■	■		■				■	■	■	■				■	■		■	

Totale caselle grigie = 50 / Totale caselle = 100

DENSITA' 50%

MACRO	FAMIGLIA	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)	(18)	(19)	(20)	(21)	(22)	(23)	(24)	(25)
CARGO MANAGEMENT	inspection during the shipping process		■					■	■			■			■	■						■		■	■	
	cargo tracking and identification technical solutions	■	■	■	■	■	■	■	■			■	■	■	■	■	■					■	■	■	■	■
	vehicle anti-tampering solutions		■					■	■			■			■			■							■	
	route management	■	■	■			■		■					■	■	■		■			■		■		■	
	ILU inspection solutions	■	■		■		■	■	■			■		■	■	■	■	■				■	■	■	■	
	ILU anti-tampering solutions	■	■	■	■	■	■	■	■			■		■	■	■	■	■	■		■	■	■		■	

Totale caselle grigie = 82 / Totale caselle = 150

DENSITA' 55%

MACRO	FAMIGLIA	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)	(18)	(19)	(20)	(21)	(22)	(23)	(24)	(25)
INFORMATION MANAGEMENT	quality information/data	■	■			■			■					■	■	■	■						■		■	
	protection of business information/data		■		■				■					■	■	■	■	■								
	recordkeeping of information	■	■		■				■		■				■	■						■		■	■	■

Totale caselle grigie = 29 / Totale caselle = 75

DENSITA' 39%

Tabella 28: Calcolo della densità per Business Network & Company Management System, Human Resource Management e Awareness Management

MACRO	FAMIGLIA	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)	(18)	(19)	(20)	(21)	(22)	(23)	(24)	(25)
BUSINESS NETWORK & COMPANY MANAGEMENT SYSTEM	company security management system	■	■		■		■	■	■	■	■	■		■	■	■	■	■		■	■	■	■	■	■	
	logistic system design	■			■		■		■	■					■					■		■		■	■	
	business partner evaluation system	■	■		■		■		■			■		■							■		■		■	
	collaborative relationship with partner and administration	■	■		■		■	■	■	■	■				■	■	■			■		■	■	■	■	■

Totale caselle grigie = 57 / Totale caselle = 100

DENSITA' 57%

HUMAN RESOURCE MANAGEMENT	employee hiring and screening process	■	■	■	■		■		■		■				■	■	■	■						■		
	employe exit process														■	■									■	
	organizational roles and responsibilities		■		■		■		■	■	■				■	■								■		

Totale caselle grigie = 24 / Totale caselle = 75

DENSITA' 32%

AWARNESS MANAGEMENT	awareness of procedures adopted by business partner			■					■	■					■	■		■		■		■		■	■	
	personnel education and training		■	■	■				■		■			■	■	■		■				■		■		
	security awarness development	■			■				■	■	■					■				■		■		■	■	

Totale caselle grigie = 31 / Totale caselle = 75

DENSITA' 41%

Il risultato dell'analisi è il seguente:

- Facility management: 50%;
- Cargo management: 55%;
- Information management: 39%;
- Business network & company management system: 57%;
- Human resource management: 32%;
- Awareness management: 41%.

Si osserva come gli strumenti di information management, human resource management e awareness management siano meno citati in letteratura rispetto alle restanti famiglie.

3.3.2 Analisi prestazioni

In Tabella 29 abbiamo riassunto tutte le informazioni ricavate dall'analisi della letteratura relativa agli impatti diretti degli strumenti sulle prestazioni individuate nel paragrafo 2.3.4; ci riferiremo quindi alle prestazioni di sicurezza preventiva, resilienza, trasparenza ed efficienza.

Tutti i legami con le prestazioni sono già stati discussi contestualmente alla descrizione degli strumenti. Non sempre è stato possibile ricavare l'informazione puntuale dell'impatto del singolo strumento sulla prestazione, mentre nella maggior parte degli articoli vengono evidenziati gli impatti relativi alle famiglie di strumenti nel loro complesso.

Per quanto riguarda le prestazioni di efficienza, gli impatti sono stati considerati sulla base di un'analisi su costi e benefici: se la famiglia di strumenti genera risparmi di costo (diretti, operativi e opportunità) esso impatta positivamente sulla prestazione (↑); se la famiglia di strumenti genera inefficienze nel processo esso impatta negativamente sulla prestazione (↓); se la famiglia di strumenti non genera inefficienze o vantaggi di costo nel processo, esso viene considerato al netto dei costi di investimento e non ha alcun impatto sulla prestazione (−).

Tabella 29: Impatti sulle prestazioni delle famiglie di strumenti

Macro	Famiglia	Sicurezza preventiva	Resilienza	Trasparenza	Efficienza
FACILITY MANAGEMENT	warehouse/terminal layout design	↑			↑/–
	facility protection	↑			↑
	facility monitoring	↑			↑
	access/presence control processes and technologies	↑			↑
CARGO MANAGEMENT	inspection during the shipping process	↑	–	↑	–
	cargo tracking and identification technical solutions	↑	↑	↑	↑
	vehicle anti-tampering solutions	↑	–		↑
	route management	↑	↑	↑	↑↓
	ILU inspection solutions	↑	–	↑	↓
	ILU anti-tampering solutions	↑	–	↑	↑/–
INFORMATION MANAGEMENT	quality information/data	↑	↑	↑	↑
	protection of business information/data	↑	–		↓
	recordkeeping of information	↑	↑		
BUSINESS NETWORK & COMPANY MANAGEMENT SYSTEM	company security management system	↑	↑	↑	↑
	logistic system design	↑	↑	↑	↑↓
	business partner evaluation system	↑	↑		↑
	collaborative relationship with partner and administration	↑↓	↑	↑	↑
HUMAN RESOURCE MANAGEMENT	employee hiring and screening process	↑			
	employe exit process	↑			
	organizational roles and responsibilities	↑	↑		
AWARNESS MANAGEMENT	awareness of procedures adopted by business partner	↑	↑	↑	
	Personnel education and training	↑	↑		
	Security awarness development	↑	↑		

Legenda:

↑ la famiglia di strumenti impatta positivamente sulla prestazione

↓ la famiglia di strumenti impatta negativamente sulla prestazione

– la famiglia di strumenti non impatta sulla prestazione

Dalla Tabella 29 si nota come ci siano due categorie di strumenti che non sono state analizzate in relazione alle prestazioni di efficienza da nessun autore: la prima riferita alla protezione fisica basilare delle strutture logistiche (facility protection, facility monitoring e access/presence control processes and technologies); la seconda riferita alla gestione delle risorse umane, della loro conoscenza e consapevolezza (recordkeeping of information, employee hiring and screening process, employe exit process, organizational roles and responsibilities, awareness of procedures adopted by business partner, personnel education and training e security awarness development). La motivazione per la prima categoria è abbastanza evidente trattandosi di strumenti di prima necessità per la protezione delle strutture da possibili attacchi, da integrare nel progetto delle strutture a prescindere da eventuali analisi di costi e benefici che possono portare. Per la seconda categoria, in accordo a Quinn (2003), la motivazione probabilmente è riconducibile al fatto che la maggior parte degli strumenti non sono direttamente collegabili alle prestazioni organizzative, oltre al fatto che, come abbiamo visto in precedenza, esiste poca letteratura su queste famiglie di strumenti.

3.4 Conclusioni

Lo scopo di questo capitolo è stato quello di effettuare una panoramica completa su quelli che possono essere i possibili strumenti che concorrono all'aumento della sicurezza. La classificazione a cui siamo giunti raccoglie tutti gli strumenti identificati in letteratura raggruppati in famiglie (da noi proposte) di strumenti simili con applicazione nello stesso ambito aziendale. Ci siamo imbattuti in articoli che trattano specifiche categorie di strumenti e articoli che invece effettuano una panoramica su tutte le possibili categorie. Questi articoli che forniscono un approccio completo e toccano a 360 gradi tutti gli aspetti della SCS si focalizzano maggiormente sulle categorie di Facility, Cargo e Business network and company management system trattando solo in modo marginale le restanti categorie. A seguito delle analisi sulla densità effettuate abbiamo avuto la conferma che solo pochi articoli approfondiscono le categorie di information, human resource e awareness mangement. In ultima istanza abbiamo cercato di riassumere quelli che sono i possibili legami tra le famiglie di strumenti proposte e le prestazioni di sicurezza preventiva, resilienza, trasparenza ed efficienza. Tutte queste informazioni saranno utili nel capitolo 4 per definire lo scopo e l'ambito della nostra ricerca.

4 Disegno di ricerca

Con il termine disegno di ricerca intendiamo la stesura di un piano che espliciti chiaramente la definizione dell'oggetto di indagine e delle attività che consentiranno di sviluppare un progetto di ricerca all'interno del contesto prescelto.
A partire dalle considerazioni emerse sugli strumenti di sicurezza, definiremo quindi lo scopo della ricerca, individuando l'ambito e le categorie di strumenti da approfondire.
Delimiteremo l'oggetto di indagine a cinque domande di ricerca e costruiremo un modello teorico nel quale è possibile includere una analisi di tipo empirico.

4.1 Definizione dello scopo e dell'ambito di ricerca

A seguito delle analisi presenti nel paragrafo 3.3 abbiamo deciso di approfondire gli strumenti appartenenti alle categorie di information, human resource e awareness per diverse ragioni. In primo luogo, come evidenziato dall'analisi delle densità nel paragrafo 3.3.1 questi strumenti risultano poco trattati in letteratura rispetto agli strumenti più classici utilizzati principalmente per il miglioramento delle prestazioni di sicurezza. Anche per quanto riguarda gli impatti sulla prestazione di sicurezza, come sottolineato nel paragrafo 2.3.4, non esistono studi quantitativi a sostegno. Abbiamo deciso quindi di approfondire lo studio di queste famiglie di strumenti, oltre che per le motivazioni appena esposte, anche per il fatto che questi, a differenza di tutti gli altri, non sono legati a specifici processi o punti all'interno della filiera del trasporto intermodale, ma sono di tipo più trasversale perché strettamente legati al fattore umano.
Quest'ultimo è molto importante per la prestazione di sicurezza: come afferma Lacey (2010) *"le azioni condotte dalle persone non sono la sola causa degli incidenti*[19]*, ma sono anche il mezzo primario per prevenire, individuare e risolvere problemi"*.
Abbiamo definito gli strumenti in questione di tipo culturale perché agiscono su valori, motivazioni, atteggiamenti e comportamenti degli individui all'interno dell'organizzazione, in accordo con la definizione di cultura organizzativa: *"la struttura di valori condivisi e credenze che aiutano gli individui a capire il funzionamento dell'organizzazione e perciò fornir loro le norme per il comportamento all'interno dell'organizzazione"* (Desphande e Webster, 1989).

[19] Con incidente intendiamo il manifestarsi dell'evento di rischio, o evento indesiderato, che può essere anche la causa di disruption

Riteniamo quindi interessante approfondire questa tematica per capire se questi strumenti culturali vengono applicati in azienda con specifici obiettivi di sicurezza e se queste ne riconoscono gli impatti.

Successivamente andremo a studiare come il concetto di cultura organizzativa si declina nelle pratiche di supply chain security

Inoltre, come evidenziato dalla analisi del paragrafo 3.3.2 (Tabella 29), queste famiglie di strumenti non presentano delle relazioni con le altre prestazioni di trasparenza ed efficienza. Lo spunto per una successiva ricerca può essere quello di indagare sugli impatti collaterali che questi strumenti possono avere sulle altre prestazioni prese in esame nel paragrafo 2.3.4.

4.1.1 Cultura organizzativa

La cultura organizzativa ha subito nel corso degli anni un crescente interesse da parte delle organizzazioni e di ricercatori. In termini molto semplici secondo McAfee et al. (2002) la cultura organizzativa si riferisce alla personalità dell'azienda. Più nello specifico è *"la struttura di valori condivisi e credenze che aiutano gli individui a capire il funzionamento dell'organizzazione e perciò fornir loro le norme per il comportamento all'interno dell'organizzazione"* (Desphande e Webster, 1989).

Un contributo importante è stato offerto da Edgar Schein (1992), che definisce la cultura come *"un insieme di assunti di base – inventati, scoperti o sviluppati da un gruppo determinato quando impara ad affrontare i propri problemi di adattamento con il mondo esterno e di integrazione al suo interno – che si è rivelato così funzionale da essere considerato valido e, quindi, da essere indicato a quanti entrano nell'organizzazione come il modo corretto di percepire, pensare, e sentire in relazione a quei problemi."*

In altre parole la cultura è data da una serie di elementi che si consolidano in un gruppo o in un'organizzazione in base alle esperienze di successo che hanno segnato il gruppo.

Schein individua tre livelli di cultura, indicati in Figura 39. Con il termine livello egli si riferisce al *"grado con cui un fenomeno culturale è visibile all'osservatore".*

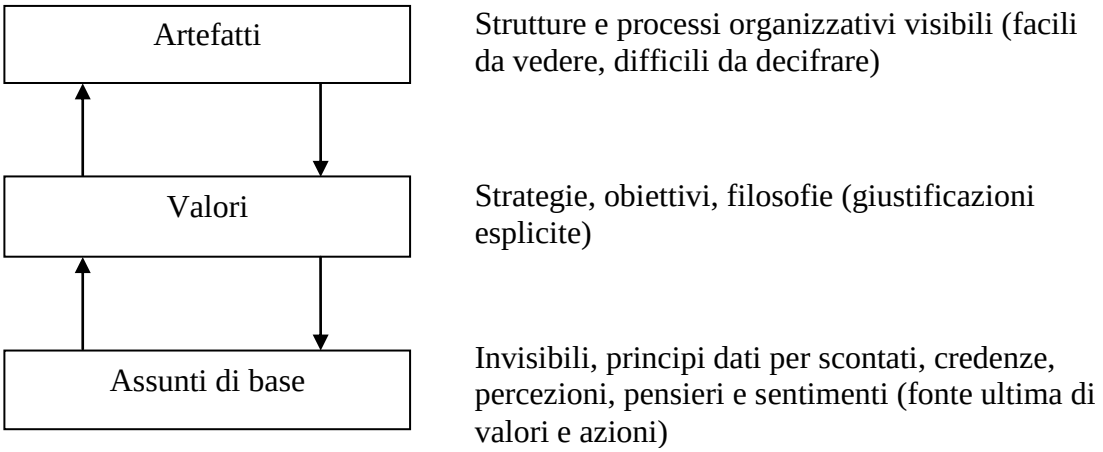


Figura 39: Livelli culturali di Schein (1992)

Al primo livello ci sono gli artefatti: sono il livello più visibile della cultura, ma difficili da decifrare. Comprendono gli elementi visibili di un'organizzazione (strutture, processi, ambiente).

Al secondo livello ci sono i valori: rappresentano le strategie, gli obiettivi e le filosofie; sono verificabili nell'ambiente fisico solamente con il consenso sociale. Solo se una soluzione ad un problema è considerata efficace con continuità da tutto il gruppo allora si innesterà un processo di trasformazione cognitiva che la renderà un assunto di base.

Infine, al terzo livello, troviamo gli assunti di base: sono il livello più profondo; sono dati per scontati e sono invisibili. Corrispondono ad assunti impliciti che determinano il comportamento, che indicano ai componenti del gruppo come la realtà vada percepita, pensata, sentita.

Questo schema dimostra che la cultura all'interno di un'organizzazione o gruppo può essere trovata a vari livelli: quello più apparente, che può essere rilevato dall'osservatore esterno (artefatti), quello che può essere registrato dalle dichiarazioni di chi vive il gruppo/organizzazione (valori) ed un livello ancora più profondo, ma più importante, che spesso non è evidente neanche a chi vive quella cultura (assunti di base).

La cultura organizzativa è stata studiata da molti ricercatori anche a livello di supply chain, i quali hanno riconosciuto l'importanza di questo tema in relazione alle tematiche di SCM. (Williams et al., 2009). In questo ambito è stato portato alla luce come la cultura sia in grado non solo di capire e definire il modus operandi di un'organizzazione, ma anche di attraversare i confini aziendali ed influenzare tutta la rete inter-aziendale. Tan et al. (1998) hanno suggerito che la cultura organizzativa è uno degli elementi più critici che i membri di una supply chain devono affrontare per

ottimizzare le performance individuali, ma anche globali. McAfee et al. (2002) affermano che per ottenere partnership di successo e una supply chain performante è necessario avere coerenza tra cultura interna a livello aziendale e cultura esterna a livello di supply chain; tale coerenza tra le culture, secondo Jia e Rutherford (2010), permette di ridurre il Supply Chain Relational Risk (SCRR), definito come *"il rischio di una supply chain che qualche parte della relazione cliente-fornitore non sia completamente coinvolta negli sforzi congiunti per la risoluzione di qualsiasi problema di cooperazione o problema associato ad un comportamento opportunistico"*. Shub e Stonebraker (2009) individuano alcuni strumenti efficaci che favoriscono l'adozione di un orientamento comune in tutta la supply chain, per la maggior parte associabili a "strumenti soft" per le risorse umane e variabili organizzative.

Molti autori individuano nella cultura un fattore critico di successo di un'organizzazione (McAfee et al., 2002; Jia e Rutherford, 2010; Sambasivan e Jen, 2010). In quest'ottica, Mello e Stank (2005), sono stati i promotori di ricerche focalizzate sul rapporto tra cultura e SCM ed hanno dimostrato che un determinato orientamento culturale promuove la realizzazione di strategie di SCM di successo; in aggiunta, hanno evidenziato che le strategie di SCM variano al variare dell'orientamento. A dimostrazione di questa tesi, e ricollegandoci al nostro ambito d'interesse, Closs e McGarrell (2004) nelle loro ricerche sulla SCS, hanno effettivamente osservato che l'adozione di determinate strategie indirizzate alla sicurezza della supply chain derivano da una cultura organizzativa orientata alla sicurezza.

4.1.2 Supply Chain Security Culture

"La Supply Chain Security Culture (SCSC), è definita come la filosofia globale di un'organizzazione che vede la sicurezza della supply chain come una priorità che deve essere riconosciuta dai suoi dipendenti e che deve manifestarsi attraverso l'adozione e la progettazione di norme e valori utili per garantire supporto ad attività sicure e l'attenzione agli sforzi per la sicurezza". (Williams et al., 2009)

Lo sviluppo di una supply chain security culture (SCSC), è diventato importante per varie ragioni, tra cui il crescente focus verso le tematiche di SCS da parte delle autorità governative e le organizzazioni private (discusso nel paragrafo 3.1), l'importanza del ruolo che le tematiche culturali ricoprono nell'influenza di obiettivi strategici, tattici e operativi delle aziende e delle supply chain (paragrafo 4.1.1) e la maggior consapevolezza che le persone di un'organizzazione e le organizzazioni stesse siano i

principali responsabili delle disruption, come vedremo successivamente nel paragrafo 4.1.3.

Con il proposito di promuovere una cultura di sicurezza, molti ricercatori hanno rivolto particolare interesse verso l'interfaccia tra SCS e le tematiche sul comportamento organizzativo.

Alcune ricerche inerenti alla SCS hanno evidenziato l'importanza degli atteggiamenti delle persone, delle pratiche di HR e di altre questioni sempre relative alle persone nella creazione di un ambiente di Supply Chain Management focalizzato sulla sicurezza (Williams et al., 2009; Rice e Spayd, 2005).

Tra gli autori che per primi hanno fornito contributi significativi per lo sviluppo di un orientamento culturale alle tematiche di sicurezza, troviamo Sheffi (2001) e Rice e Caniato (2003).

Sheffi (2001), nel suo articolo "Supply Chain Management under the Threat of International Terrorism", propone nuove sfide per la gestione della supply chain, pensate in seguito all'attacco terroristico dell'11 settembre. Oltre a proporre molteplici strategie di business, Sheffi affronta in modo diretto il tema della cultura, affermando che *"nessun Chief Security Officer o Security Organization avrà successo senza che la cultura di impresa promuova la consapevolezza sulla sicurezza nella quotidianità". Perciò, le imprese che sopravvivranno agli attacchi terroristici saranno quelle i cui dipendenti abbiano interiorizzato un set di misure intelligenti di sicurezza".*

Rice e Caniato (2003), hanno condotto un'indagine tra le supply chain globali per studiare l'efficacia nell'implementazione di strumenti per la sicurezza e la resilienza di una supply chain. Un importante gruppo di strumenti da loro individuati favoriscono quella che loro definiscono *"la "socializzazione" della sicurezza e resilienza"* e sono tali da *"far diventare sicura e resiliente una parte della cultura organizzativa"*. Nella loro ricerca hanno messo in luce l'importanza di avere una cultura che permetta alle supply chain di essere proattiva e attenta ai rischi che possono correre in modo da perseguire gli obiettivi di SCS e *"costruire una supply chain sicura e resiliente*". In particolare, secondo Rice e Caniato, la cultura di sicurezza può essere raggiunta attraverso un programma intensivo di formazione e istruzione alle risorse umane.

Lo stesso tema della *"socializing security"* è stato portato avanti da Rice e Spayd (2005), i quali sostengono che ha l'obiettivo dello sviluppo della consapevolezza della sicurezza tra gli individui di una supply chain attraverso la cultura organizzativa. Inoltre individuano la struttura organizzativa, la leadership, le abilità degli individui e la

formazione del personale sulle questioni di sicurezza come i principali fattori coinvolti in questo processo di socializzazione.

Più recentemente, Williams et al. (2008) sottolineano che un fattore critico di successo per la SCS è proprio quello di creare e supportare una cultura organizzativa che permetta alle supply chain di percepire l'importanza della sicurezza per la continuità del business e le sue operation.

A supporto di questa tesi, Autry e Bobbitt (2008), osservando i risultati dei dipendenti nello svolgimento dei compiti giornalieri, hanno dedotto che le aziende i cui dipendenti manifestavano un atteggiamento orientato alle questioni di SCS potevano beneficiare di parecchi vantaggi in termini di performance organizzative. Dai loro studi risulta che le aziende possono avere diversa consapevolezza alla SCS. Tale variazione nella "mentalità" delle organizzazioni viene chiamata Supply Chain Security Orientation (SCSO), definita come *"la propensione di un'organizzazione a pianificare, adattarsi, collaborare e comunicare, sia internamente che esternamente, con i partner e gli enti governativi, attraverso entrambi gli obiettivi di prevenzione strategica e di risposta alle potenziali debolezze e attraverso la minimizzazione del rischio che minaccia le performance e/o la continuità del business della supply chain".* La SCSO prevede un approccio sia intra-organizzativo che inter-organizzativo alla sicurezza (Williams et al., 2008), in cui la decisione di orientare le risorse alla SCS deve essere presa congiuntamente dalle componenti di una supply chain (Closs e McGarrell, 2004). Williams et al. (2008) mostrano che spesso all'approccio di SCSO vengono associate per analogia filosofie di continuous improvement e di Total Quality Management (TQM), adattate alla sicurezza. In accordo all'idea di Williams et al., Lee e Wolfe (2003) dimostrano che i principi del TQM possono effettivamente essere applicati in ottica della sicurezza e favorire la creazione di una supply chain resiliente e sicura. Alcuni di questi principi, infatti, come affermano gli autori, comprendono la prevenzione, il disegno di piani di sicurezza, il controllo sui processi di sicurezza e il focus sull'intero processo di creazione del valore della supply chian.

Infine, un contributo rilevante per il nostro lavoro è stato fornito da Benson (2005) che ha analizzato il ruolo della cultura organizzativa nella creazione di una supply chain sicura e resiliente. Nel suo lavoro, Benson ha illustrato i fattori chiave di successo per la creazione di una "cultura di sicurezza" e ha proposto un framework, ispirato ai livelli della cultura di Schein (vedi paragrafo 4.1.1), per gli strumenti che aumentano le performance di sicurezza e resilienza di una supply chain; tale framework ci ha aiutato

nella formulazione di uno schema mentale per il riconoscimento di strumenti di tipo culturale, descritti nel paragrafo 4.3.2.

4.1.3 Cultura di sicurezza e fattore umano

"Non esiste un mondo senza errori; gli uomini trascorrono la maggior parte della loro vita nelle organizzazioni o in contesti organizzati, per cui la maggior parte dei casi gli errori possono essere riferiti a dinamiche organizzative". (Catino, 2002)

"Le azioni condotte dalle persone non sono la sola causa degli incidenti[20]*, ma sono anche il mezzo primario per prevenire, individuare e risolvere problemi"* (Lacey, 2010).

Tenendo presente questi rischi e opportunità non è sufficiente focalizzarsi solo sulle classiche procedure di sicurezza e le tecnologie che abbiamo visto negli strumenti di sicurezza e interessano il livello fisico dell'infrastruttura e dell'organizzazione; ma "*è necessario un intervento che porti al cambiamento della consapevolezza, atteggiamenti e comportamenti delle persone"*, come afferma Lacey (2010).

Entrambi gli autori affermano che queste considerazioni hanno portato le aziende ad affrontare la sicurezza attraverso una forte attenzione alla "cultura di sicurezza".

Lacey (2010) evidenza come la scelta di adottare una cultura rivolta alla sicurezza non sempre porti ad una soluzione univoca. Ad esempio, egli mostra che è possibile fondare la cultura su motivazioni negative, come la paura e paranoia, attraverso punizioni oppure su motivazioni positive come la fiducia e la responsabilizzazione, attraverso premi e riconoscimenti. Nella maggior parte dei casi, la natura di una cultura di sicurezza è determinata dalle reazioni del management agli incidenti e conseguenti disruption. Partendo da un'analisi delle possibili risposte dei manager, Lacey (2010) dimostra come una cultura fondata sulla paura sia fallimentare. Anzitutto, *"tale cultura spinge di più alla ricerca di un colpevole piuttosto che all'analisi delle vere cause di un evento indesiderato"*. Di conseguenza, essendo gli incidenti per la maggior parte dei casi il risultato di una combinazione di fattori piuttosto che dall'azione di una singola persona, la ricerca di un colpevole potrebbe mettere in ombra ragioni ben più profonde che hanno causato l'incidente. In definitiva questo non permette di eliminare gli errori dovuti, ad esempio, ad un carico di lavoro troppo elevato oppure a controlli e procedure inadeguate. Lacey conclude dicendo che *"il risultato che si ottiene è lo sviluppo di una*

[20] Con incidente intendiamo il manifestarsi dell'evento di rischio, o evento indesiderato, che può essere anche la causa di disruption

"cultura dell'accusa" che danneggia la cooperazione, scoraggia le persone ad affrontare i rischi e a riportare informazioni, incidenti e near misses".

Dall'altro canto, Lacey (2010) sostiene che *"una sana cultura "no-blame" basata sulla fiducia e sulla responsabilizzazione ha più probabilità di portare risultati virtuosi e duraturi. […] Essa genera una fondata consapevolezza sulla sicurezza, la volontà di denunciare debolezze o punti deboli, la franchezza nelle valutazioni di conformità della sicurezza e un grado di empowerment che consenta al personale di adottare misure correttive"*. Il tema della responsabilizzazione (traduzione del termine inglese "empowerment") è stato approfondito da molti autori in riferimento alla cultura di sicurezza: Autry e Bobbitt (2009) individuano nell'empowerment il chiaro risultato di una Supply Chain Security Culture; Sheffi (2005c) invece riporta alcuni esempi di organizzazioni che hanno applicato una cultura di successo basata sulla responsabilizzazione come Nokia, Toyota, UPS, Schneider National, FedEx, Dell, e US Navy.

Dal precedente discorso emerge l'importanza di un'analisi approfondita della natura degli incidenti di un'organizzazione, in quanto consente di conoscere molti aspetti non comunemente osservabili nel loro funzionamento "normale".

Le cause degli incidenti, come abbiamo visto, non sempre sono attribuite a un singolo individuo. A tal proposito Lacey (2009) afferma che *"è interessante osservare che la maggior parte degli errori che causano la maggior parte degli eventi indesiderati, sono causati da fattori umani non associati a un comportamento negativo. Fattori come stress, mancanza di training o supervisione e sistemi mal progettati sono spesso la causa degli attuali buchi di sicurezza"*. Lo stesso Catino (2002), afferma che *"gli incidenti non sempre sono il frutto di una sola persona (o di un team di lavoro), ma talvolta posso essere determinati dal progressivo accumularsi di carenze e manchevolezze da parte di chi dirige e gestisce la struttura organizzativa"*. Queste considerazioni devono spingere ancora di più il management ad adottare una cultura della sicurezza, con una forte attenzione alle cause che stanno alla radice degli incidenti.

Un approfondimento sulla metodologia di valutazione degli incidenti secondo un'opportuna cultura di sicurezza "no-blame", è stato fornito da Catino (2002) che individua nell'utilizzo congiunto dell' *"approccio alla persona"* e dell' *"approccio al sistema"* la soluzione ottimale per una corretta valutazione. Il primo tiene conto di eventuali errori o eventi indesiderati causati da comportamenti negativi del singolo individuo (o gruppo) e trova la soluzione ai problemi che intaccano la sicurezza tramite

la rimozione degli stessi individui dall'organizzazione; il secondo considera *"fattori critici latenti che predispongono all'errore"* e si focalizza sul sistema trovando la soluzione nel miglioramento dell'organizzazione complessiva, tenendo conto anche dei "fallimenti" a livello inter-organizzativo (*"coordinamento tra gli enti coinvolti, regole non chiare, rapporto critico tra controllante e controllata, pressioni all'efficienza non integrate con la sicurezza"*). Nell'approccio al sistema, Catino tiene conto di molteplici fonti d'errore umano: *"la capacità di lavoro limitate, incapacità di mantenere l'attenzione per lunghi periodi, approcci mentali poco flessibili, capacità d'elaborazione dati solo se in riferimento alla propria cultura professionale"* basandosi su alcuni principali modelli sociologici sull'errore umano di Reason (1990) e Rasmussen (2000).

4.2 Domande di ricerca

Dato l'ambito e la tematica di interesse esposta nel paragrafo 4.1 abbiamo esplicitato i nostri obiettivi di ricerca sintetizzandoli in 5 domande:

1. Quali strumenti culturali sono adottati nelle aziende del settore intermodale?
2. Qual è l'impatto che l'applicazione di ogni strumento ha sulla prestazione di sicurezza?
3. Esistono dei fattori di contesto che spiegano l'adozione degli strumenti culturali?
4. I fattori di contesto spiegano anche gli impatti degli strumenti sulle prestazioni?
5. Quali sono le cause più importanti che determinano una cattiva prestazione di sicurezza? Sono diverse in funzione dei fattori di contesto?

Queste problematiche saranno la nostra linea guida per impostare tutte le attività che seguiranno: dalla formulazione di un modello teorico all'individuazione dell'unità di analisi (le aziende campione), fino alla creazione degli strumenti per la raccolta e l'analisi dei dati.

4.3 Modello teorico

Descriveremo in questo capitolo il modello teorico da noi elaborato per dare una risposta, che sarà poi da verificare ed approfondire tramite l'analisi dei dati, alle domande di ricerca espresse nel paragrafo 4.2. Questo sarà di fondamentale importanza

per guidare la raccolta delle informazioni e stabilire le fonti più idonee per raggiungere i nostri scopi di analisi.

Abbiamo individuato un framework di analisi (Figura 40) che comprende i seguenti aspetti:

- Fattori di contesto
- Strumenti culturali
- Fattori causa
- Prestazioni di sicurezza

Per la spiegazione nel dettaglio dei sopracitati aspetti del framework si rimanda ai paragrafi seguenti.

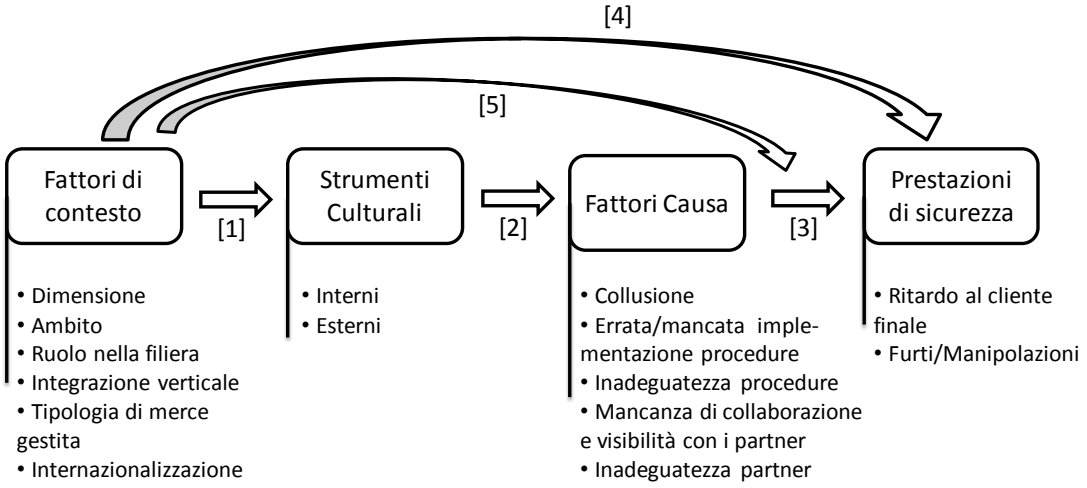


Figura 40: Modello teorico

Il modello teorico da noi elaborato riguarda le possibili relazioni schematizzate in Figura 40. Riteniamo che i fattori di contesto possano spiegare l'impiego di particolari tipologie di strumenti. Riteniamo cioè, ad esempio, che la dimensione di un'azienda sia una discriminante nell'utilizzo di un particolare strumento culturale. Questo tipo di relazione tra fattori di contesto e strumenti culturali è espressa dalla freccia [1].

La seconda relazione, che coinvolge gli strumenti culturali e i fattori causa, indica invece il possibile impatto del singolo strumento culturale su uno specifico fattore causa. A nostro avviso ogni strumento può quindi impattare su diversi fattori causa in modo più o meno marcato (ad esempio la lealtà dei dipendenti è uno strumento che ci aspettiamo ridurrà il fattore causa collusione).

La relazione che intercorre tra i fattori causa e la prestazione di sicurezza è invece modellizzata dalla freccia [3]; come analizzeremo nel paragrafo 4.3.4. la prestazione di sicurezza deriva dal verificarsi di determinate cause (i fattori causa appunto).

Viene poi rappresentata, tramite la freccia [4], la relazione che intercorre tra i fattori di contesto di un'azienda e i relativi impatti degli strumenti sulla sicurezza (così da poter rispondere alla domanda di ricerca n° 4). Ci aspettiamo cioè che in funzione dei fattori di contesto gli impatti degli strumenti sulla prestazione di sicurezza possano essere differenti.

La freccia [5] rappresenta invece la risposta alla domanda di ricerca n°5, ovvero determina l'importanza relativa dei fattori causa in base ai fattori di contesto.

Di seguito illustreremo nel dettaglio i quattro blocchi in Figura 40.

4.3.1 Fattori di contesto

Sulla base delle informazioni ricavate dalla letteratura analizzata nel paragrafo 2.4.1 sulla vulnerabilità delle ILU supply chain ed in base ad alcune nostre considerazioni, abbiamo identificato alcune variabili che possono giustificare l'utilizzo di uno strumento (relazione [1]), determinarne il maggiore o minore impatto sulla prestazione di sicurezza (relazione [4]) o eventualmente il diverso impatto sui fattori causa (relazione [5]). Queste variabili che permettono di distinguere il profilo di un'azienda sono i fattori di contesto approfonditi di seguito.

Dimensione azienda

La dimensione di un'azienda è un fattore che può far riferimento a diversi aspetti. Generalmente misura il grado di attività aziendale, ossia il livello produttivo
delle aziende, ma può assumere significati diversi in base alle analisi che si vogliono condurre. Nella nostra analisi prenderemo come riferimento la Raccomandazione della Commissione Europea 6 maggio 2003, n. 2003/361/Ce, recepita a livello nazionale dal DM 18 aprile 2005, che determina la dimensione aziendale sulla base del numero di dipendenti, espressi in unità lavorative annue (ULA), del fatturato o del totale di bilancio, come illustrato in Tabella 30.

Tabella 30: Parametri per la determinazione della dimensione aziendale

	Dipendenti (ULA)	Fatturato (milioni di euro)	Totali di bilancio (milioni di euro)
Micro impresa	Inferiore a 10	Fino a 2	Fino a 2
Piccola impresa	Da 10 a 49	Oltre i 2 e fino a 10	Oltre i 2 e fino a 49
Media impresa	Da 50 a 249	Oltre i 10 e fino a 50	Oltre i 10 e fino a 43
Grande impresa	Da 250	Oltre i 50	Oltre i 43

Per il nostro scopo riteniamo tuttavia che il fatturato (o il totale di bilancio) non siano elementi che possano avere forti relazioni con le pratiche di natura culturale e organizzativa di cui ci occuperemo, per cui la determinazione della dimensione aziendale sarà riferita prevalentemente al numero di dipendenti. In questi termini la dimensione aziendale è una chiara proxy del livello di strutturazione organizzativa. Nella struttura organizzativa vengono inclusi i concetti di divisione del lavoro, team working, meccanismi di coordinamento e decentramento. È corretto quindi pensare che un'organizzazione con un numero maggiore di dipendenti presenti un maggior numero di meccanismi di gestione del lavoro e di politiche di gestione delle risorse umane e quindi una maggiore strutturazione. Per questo motivo riteniamo che la dimensione, sia un fattore altamente discriminante nell'adozione di alcune politiche gestionali e culturali che agiscono su aspetti della sicurezza in cui il fattore umano è la determinante di una buona o cattiva prestazione.

Ambito

Si riferisce al settore di appartenenza: ferrovia o strada. Gli attori che si occupano della tratta del trasporto solo su strada o solo su ferrovia, mostrano criticità diverse, trattandosi difatti di due realtà ben distinte. In riferimento allo schema proposto da Sarathy (2005) sugli elementi che determinano la vulnerabilità della supply chain (paragrafo 2.4.1), si può dimostrare che tali criticità sono differenti in base all'ambito considerato: un attore che si interfaccia con la strada piuttosto che con la ferrovia vede infatti partner, strutture logistiche, tipologie di operatori e informazioni differenti, ognuna delle quali rappresenta un rischio differente. Riteniamo quindi che l'ambito possa essere una variabile determinante per capire l'adozione di alcuni strumenti da parte di un'organizzazione.

Ruolo nella filiera intermodale

Si riferisce alle responsabilità atomiche (individuate nel paragrafo 1.6) che le organizzazioni possiedono all'interno del trasporto intermodale, ossia MTO, vettore

stradale, gestore del terminal, trazionista, gestore della rete ferroviaria e operatore commerciale del trasporto ferroviario.

Un'organizzazione può assumere da un singolo ruolo a molteplici e ciascuno si riferisce a un singolo ambito del trasporto intermodale. Per questo motivo le criticità del ruolo sono strettamente legate a quelle caratterizzanti l'ambito di riferimento; in aggiunta le criticità possono variare in base alle aree di responsabilità nel trasporto. Pertanto riteniamo che, ai fini della nostra analisi, il ruolo nella filiera intermodale possa essere un fattore discriminante nell'utilizzo delle pratiche di sicurezza, che può essere studiato contestualmente all'analisi dell'ambito di riferimento.

Integrazione verticale

Con integrazione verticale si intende la capacità di un'organizzazione di integrare al suo interno un maggior numero di attività per la realizzazione di un prodotto/servizio. "*Un'azienda integrata verticalmente è unita attraverso una gerarchia e condivide un proprietario comune. Di solito ogni membro della gerarchia si occupa di attività differenti che insieme soddisfano un bisogno comune"* (Wikipedia, 2011).

Il trasporto intermodale, rispetto al trasporto monomodale rappresenta una forma di trasporto decisamente più complessa, in quanto composto da un serie di attori associati ad una o più operazioni costituenti delle catene di trasporto. In una realtà così complessa, l'interazione fra gli attori del sistema solitamente pone problemi di coordinamento delle operazioni, di controllo della catena logistica, di convivenza fra professioni e culture eterogenee, che invece non esisterebbero nelle organizzazioni di trasporto monomodale.

Debernardi (1997), in un suo intervento sulla rivista KINEO, ha illustrato quali complessità deve sostenere settore intermodale e spiegato come l'integrazione di filiera in alcuni casi sia stata implementata in risposta alle criticità spiegate sopra: *"la necessità di gestire correttamente la complessità delle nuove relazioni ha condotto molti soggetti ad aumentare la loro articolazione interna; così, ad esempio, le compagnie ferroviarie hanno dato vita, alleandosi con gruppi di spedizionieri, a imprese specializzate nella gestione del combinato strada-rotaia (Kombiverkehr in Germania, Novatrans in Francia, Cemat in Italia ecc.)"* Inoltre aggiunge che *"gli interessi di questi soggetti* (i differenti ruoli all'interno della filiera) *sono a volte convergenti e a volte divergenti"*, per cui l'integrazione può favorire una visione di filiera che difficilmente ogni singolo ruolo riuscirebbe a mettere in pratica attraverso

l'allineamento degli obiettivi. In definitiva, crediamo che il livello di integrazione verticale sia un fattore discriminante nella scelta dell'approccio alla sicurezza e degli strumenti da utilizzare da parte degli operatori intermodali; a supporto di questa considerazione si evidenzia che le aziende con un alto livello di integrazione sono in genere di grande dimensione, pertanto il fattore integrazione potrebbe avere implicazioni simili a quello della dimensione.

Tipologia di merce trasportata

Nel trasporto intermodale, l'ampia gamma di ILU a disposizione, permette il trasporto di qualsiasi tipo di merce. Queste possono essere classificate in modo differente a seconda di vari aspetti come peso, dimensione, deperibilità, pericolosità, a temperatura controllata, sfusa o pallettizzata, etc. Per la nostra analisi abbiamo definito tre categorie di merci differenti:

- merce pericolosa;
- merce ad alta appetibilità;
- merce non pericolosa e non appetibile.

La scelta di raggruppare tutte le possibili tipologie di merci in queste categorie deriva dall'influenza che esse possono avere sulla sicurezza del trasporto intermodale.

Le merci pericolose comprendono, sostanze e prodotti esplosivi, gas, liquidi e solidi infiammabili, sostanze soggette a combustione spontanea, che emettono gas infiammabili a contatto con l'acqua, sostanze ossidanti, sostanze tossiche, perossidi organici, materiali infettanti, radioattivi, sostanze corrosive e varie altre sostanze e materiali pericolosi (Daschkovska, 2010), il cui trasporto è regolamentato dalle normative ADR e RID, riferite rispettivamente al trasporto su strada e su ferrovia. I soggetti che trasportano questa tipologia di merci corrono rischi specifici, sia in termini di safety che di security, come ad esempio azioni criminali e terroristiche.

Le merci ad alta appetibilità sono invece riferite a quelle merci più soggette a furti ma anche a contaminazione nel caso di prodotti ad uso alimentare. Possono comprendere sia merci ad alto valore (high tech, rame, vestiti firmati, profumi, etc), sia merci caratterizzate da facilità di trasporto e di vendita (sigarette, liquori, food e GDO) che le rendono appetibili ai furti, mentre le merci sfuse per l'utilizzo alimentare (granaglie e liquidi) potrebbero essere soggette a contaminazione per scopi terroristici.

La merce non appetibile e non pericolose si riferisce a tutte quelle non incluse nelle categorie precedenti, ossia a basso valore, pesante, difficilmente vendibile e merce sfusa non alimentare (carta e packaging, ferro, prodotti industriali). Seppur poco appetibile ai furti e con criticità inferiori rispetto alla merce pericolosa, non può essere ritenuta completamente esente da minacce. In questa categoria rientra anche il trasporto di ILU vuote che *"devono essere soggette a controlli da parte delle autorità. […]. Questa sottocategoria di carico non può non essere considerata dal punto di vista della sicurezza. Alcuni container vuoti potrebbero essere usati dai criminali per trasportare bombe o persone illegalmente"* (Daschkovska, 2010).

Infine, come abbiamo già trattato nel paragrafo 2.4.1, ogni tipologia di merce è caratterizzata da rischi differenti a causa della differente vulnerabilità a cui è associata una tipologia di container (Crist et al., 2005). In conclusione, riteniamo che la tipologia di merce possa essere un fattore discriminante nella nostra analisi, in quanto, in base alla tipologia di merce gestita e movimentata, si possono avere implicazioni a livello gestionale e di sicurezza diverse.

Internazionalizzazione

La presenza di filiali di un gruppo o azienda all'estero, se supportata da una forte comunicazione interaziendale, potrebbe aiutare la diffusione in tutta l'organizzazione di principi provenienti da culture differenti e influenzare positivamente il modus operandi delle altre filiali. Si suppone pertanto che le aziende operanti in Italia che fanno parte di un'organizzazione estesa su scala internazionale, possano trarre beneficio dalle culture dei Paesi in cui il trasporto intermodale è più sviluppato (Svizzera, Germania, Olanda) e dove ci sia una maggior consapevolezza sull'importanza della sicurezza.

4.3.2 Strumenti culturali

Considerando il nostro ambito di ricerca riguardante la sicurezza nel trasporto intermodale (e in maniera più estesa la supply chain security) molti autori hanno descritto quali sono gli strumenti[21] da utilizzare per poter diffondere una cultura della sicurezza in azienda. Nessun autore ha però fornito una classificazione degli strumenti da utilizzare per ottenere una security culture. Con questo obiettivo, dall'analisi puntuale degli strumenti abbiamo cercato di ricavare una mappatura degli approcci alla security culture, riportata nella Figura 38. Per classificare gli strumenti ci siamo basati

[21] Il termine "strumento" è usato in senso figurato, per esprimere "ciò di cui ci si serve per ottenere qualcosa" (definizione da dizionario della lingua italiana) che in questo caso è la security culture

sulla letteratura riferita alla cultura della sicurezza. Abbiamo condotto l'analisi principalmente sulle banche dati "ISI Web of Knowledge"," Scopus", "Emerald" e "Google Scholar" ricercando le parole chiave "supply chain security culture". Questa analisi della letteratura si differenzia dalla precedende analisi sugli strumenti (capitolo 3) perché focalizzata soltanto sugli strumenti culturali all'interno delle pratiche di SCS, consentendoci quindi di raggiungere un livello di dettaglio maggiore.

Abbiamo selezionato 14 tra articoli, journal, tesi e pubblicazioni che meglio rispecchiavano i criteri di ricerca immessi e basandoci su questi abbiamo effettuato la classificazione degli strumenti.

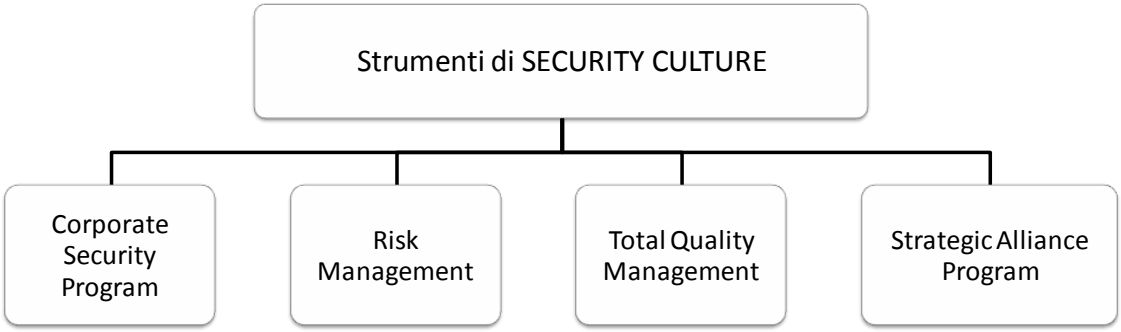


Figura 41: Classificazione degli approcci alla security culture

Ad ogni approccio riportato in Figura 41corrispondono una serie di strumenti che abbiamo ritenuto necessari per ottenere un impatto positivo sullo sviluppo di una cultura della sicurezza. Gli approcci non hanno lo scopo di suddividere in insieme distinti diverse tipologie di strumenti; è per questo motivo che uno strumento può essere funzionale a più approcci. Gli strumenti sono stati inoltre suddivisi su più livelli per evidenziarne anche le componenti più atomiche. Dalla Tabella 32 alla Tabella 34 sono riportati i legami tra gli strumenti e le fonti bibliografiche che li hanno citati come importanti per lo sviluppo della security culture.

Tabella 31: articoli sulla security culture

	Fonte bibliografica
(1)	Sheffi Y. (2001) - "Supply chain management under the threat of international terrorism", International Journal of Logistics Management (Vol. 12, No. 2, pp.1-11)
(2)	Caniato F., Rice J.B. (2003) - "Building a secure and resilient supply chain", Supply Chain Management Review (Ottobre/Novembre)
(3)	Benson S. (2005) – "The role of organizational culture in creating secure and resilient supply chains", Degrees of Master of Science in Transportation and Master of Engineering in Logistics, MIT

(4)	Mello E., Stank P. (2005) – "Linking firm culture and orientation to supply chain success", International Journal of Physical Distribution & Logistics Management (Vol. 35 No. 8, pp. 542-554)
(5)	Autry C.W., Bobbitt L.M. (2008) – "Supply chain security orientation: conceptual development and a proposed framework", The International Journal of Logistics Management (Vol. 19 No. 1, pp. 42-64)
(6)	Garrido S., Machado V.H. (2009) – "Strategies to mitigate supply chain disturbances", NECE, Department of Management and Economics University of Beira Interior, Covilhã, Portugal
(7)	Williams Z., Ponder N., Autry C.W. (2009) – "Supply chain security culture: measure development and validation", The International Journal of Logistics Management (Vol. 20 No. 2, pp. 243-260)
(8)	Shub A.N., Stonebraker P.W. (2009) – "The uman impact on SC: evaluating the importance of soft areas on integration and performance", Supply Chain Management: An International Journal (14/1/2009, pp. 31–40)
(9)	Lacey D. (2010) – "Understanding and trasforming organizational security culture", Information Management & Computer Security (Vol. 18 No. 1, pp. 4-13)
(10)	Asree S., Zain M., Razalli M.R. (2010) – "Influence of leadership competency and organizational culture on responsiveness and performance of firms", International Journal of Contemporary Hospitality Management (Vol. 22 No. 4, pp. 500-516)
(11)	Jia F., Rutherford C. (2010) – "Mitigation of supply chain relational risk caused by cultural differences between China and the West", The International Journal of Logistics Management (Vol. 21 No. 2, pp. 251-270)
(12)	Sambasivan M., Yen C.N. (2010) – "Strategic alliances in a manufacturing supply chain. Influence of organizational culture from the manufacturer's perspective", International Journal of Physical Distribution & Logistics Management (Vol. 40 No. 6, pp. 456-474)
(13)	Wu S.J., Zhang D., Schroeder R.G. (2011) – "Customization of quality practices: the impact of quality culture", International Journal of Quality & Reliability Management (Vol. 28 No. 3, pp. 263-279)
(14)	Talib F., Rahman Z., Qureshi M.N. (2011) – "A study of total quality management and supply chain management practices", International Journal of Productivity and Performance Management (Vol. 60 No. 3, pp. 268-288)

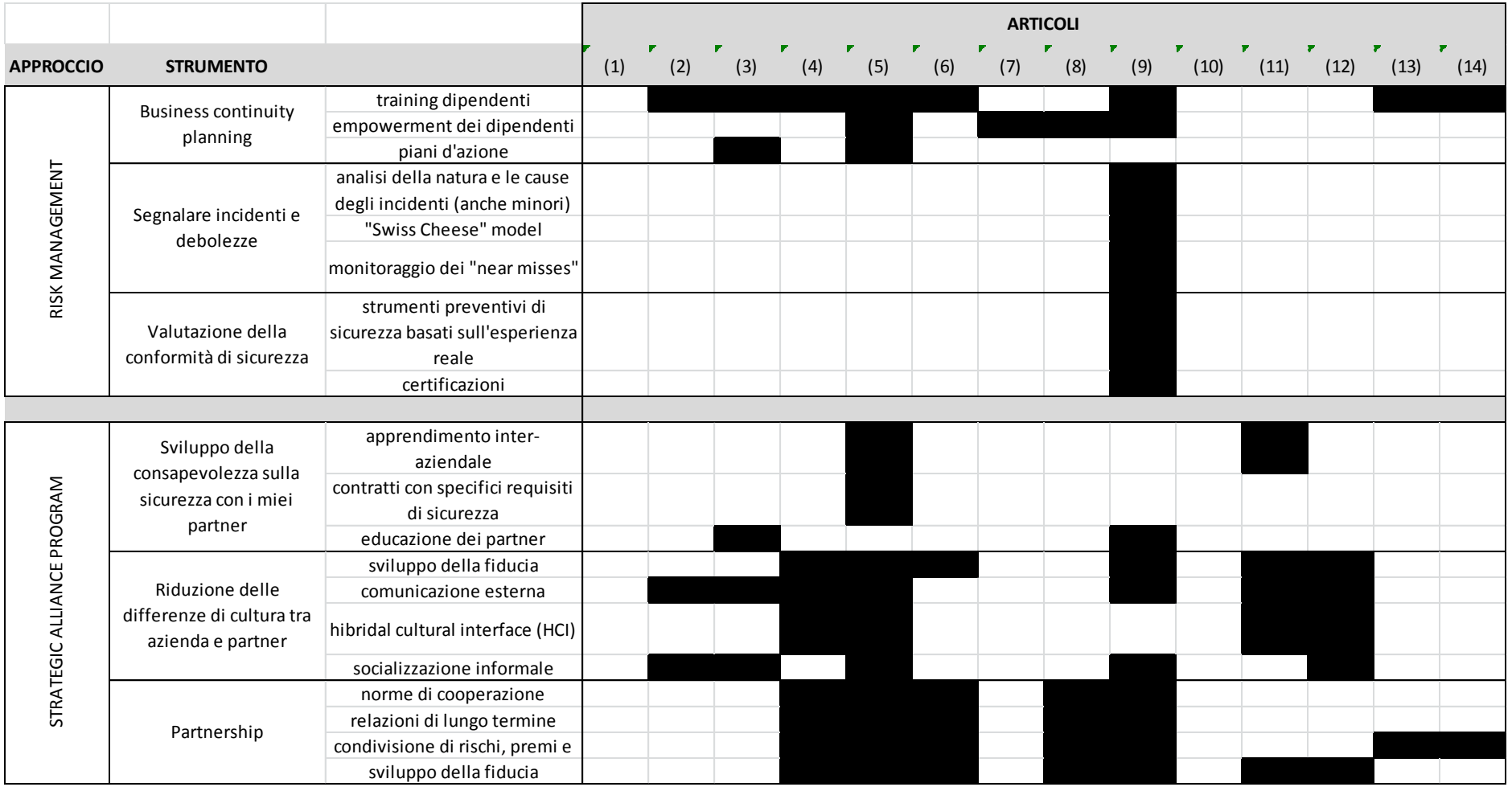
Tabella 32: Fonti bibliografiche degli strumenti culturali-Corporate Security Program

			ARTICOLI													
APPROCCIO	**STRUMENTO**		(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)
CORPORATE SECURITY PROGRAM	Integrità, lealtà dei dipendenti	investigazione sul passato e colloqui con potenziali		■	■		■									
		programmi di lealtà/fedeltà dei dipendenti					■									
		HR policy			■											
		span of control			■											
	Competenza dei dipendenti sulle tematiche di sicurezza	coinvolgimento di esperti esterni		■												
		training dipendenti		■	■	■	■	■			■				■	■
		teamwork	■	■	■						■					
	Consapevolezza interna sulla sicurezza	assegnazione responsabilità di sicurezza al personale			■		■									
		sistema di incentivazione e feedback sulla sicurezza			■		■	■			■	■				
		punizioni			■						■					
		socializzazione informale		■	■						■					
		comunicazione interna		■	■	■	■				■		■			
		funzione/posizione dedicata alla security (CSO)	■	■	■	■	■				■	■	■			■
	Aspetti soft	simbolismo												■		
		motto			■											
		codice di condotta			■											

Tabella 33: Fonti bibliografiche degli strumenti culturali-Total Quality Management

			ARTICOLI													
APPROCCIO	**STRUMENTO**		(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)
TOTAL QUALITY MANAGEMENT	Partnership	norme di cooperazione				■	■	■		■	■					
		relazioni di lungo termine				■	■	■		■	■					
		condivisione di rischi, premi e responsabilità				■	■	■		■	■				■	■
		sviluppo della fiducia				■	■	■		■	■		■	■		
	Collaborazione tra dipendenti	condivisione di rischi, premi e responsabilità				■	■	■		■	■				■	■
		teamwork			■						■				■	■
	Forza lavoro multidisciplinare	interazione cross-funzionale		■											■	
		assunzione di persone con specifiche competenze		■											■	
		training dei dipendenti		■	■	■	■	■			■				■	■
	Focus sul cliente															■
	Continuous improvement	funzione/posizione dedicata alla security (CSO)	■	■	■	■	■				■	■	■			■
		supporto del top management				■										■
		controllo dei processi esistenti													■	■
		empowerment dei dipendenti					■		■	■	■					■
	Knowledge management	apprendimento inter-aziendale	■			■	■						■	■		
		istituzionalizzazione della conoscenza					■						■			

Tabella 34: Fonti bibliografiche degli strumenti culturali-Risk Management e Strategic Alliance Program



Di seguito viene fornita una descrizione di ogni approccio alla security culture e degli strumenti che ne fanno parte.

Corporate security program

Tabella 35: Corporate security program

APPROCCIO	STRUMENTO	
CORPORATE SECURITY PROGRAM	Integrità, lealtà dei dipendenti	investigazione sul passato e colloqui con potenziali dipendenti e terze parti
		programmi di lealtà/fedeltà dei dipendenti
		HR policy
		span of control
	Competenza dei dipendenti sulle tematiche di sicurezza	coinvolgimento esperti esterni
		training dipendenti
		Team work
	Consapevolezza interna sulla sicurezza	assegnazione responsabilità di sicurezza al personale
		sistema di incentivazione e feedback sulla sicurezza
		Punizioni
		programmi di cambiamento organizzativo
		socializzazione informale
		comunicazione interna
		funzione/posizione dedicata alla security (CSO)
	Aspetti soft	simbolismo
		motto
		codice di condotta

Questo approccio porta alla definizione di un piano strutturato per lo sviluppo e la diffusione di una cultura della sicurezza in azienda. È quindi un approccio intra-aziendale rivolto all'area operativa d'azienda e che l'area manageriale deve dimostrare di supportare appieno per non ostacolarne la diffusione.

Come afferma Lacey (2009) *"la disciplina può essere raggiunta con la paura di punizioni o la promessa di una ricompensa. Alla fine del giorno, però, l'orgoglio e la gioia sono fattori più duraturi e motivanti della paura. L'ispirazione che crea la cultura organizzativa della sicurezza è una leva più potente e duratura dell'autorità".*

Gli strumenti riferiti a questo approccio sono descritti di seguito.

Integrità, lealtà dei dipendenti

Sono strumenti di selezione e affiliazione del personale. Per quanto riguarda la sicurezza preventiva, l'investigazione sul passato e i colloqui con potenziali dipendenti e terze parti rappresentano un'utile politica da adottare (per la descrizione più dettagliata si può fare riferimento allo strumento "Employee hiring and screening process" descritto nel paragrafo 3.2.7).

Gli strumenti di affiliazione, che secondo Autry e Bobbit (2008) rientrano tra i "motivatori interni" possono essere di due tipi: da un lato possono essere policy che rendono espliciti i comportamenti che l'azienda si aspetta che il dipendente abbia, ed eventualmente le punizioni alle quali questo andrà incontro se dovesse infrangere tali comportamenti. Dall'altro possono essere dei programmi che premiano la lealtà/fedeltà dei dipendenti per chi raggiunge determinati obiettivi di sicurezza o di qualità del lavoro, o di altro tipo, come incentivi economici oppure il riconoscimento di uno status[22] piuttosto che altri premi di natura non economica. In assenza di queste politiche, limitare lo span of control delle figure predisposte al controllo in azienda è uno strumento di natura organizzativa che consente di vigilare sull'integrità dei dipendenti.

Competenza dei dipendenti sulle tematiche di sicurezza

Questo strumento agisce in maniera diretta sull'aumento della competenza dei dipendenti sulle tematiche di sicurezza tramite il coinvolgimento di esperti esterni, la progettazione di team sulla sicurezza e il training dei dipendenti. Lo strumento è complementare a quello di "consapevolezza interna sulla sicurezza" (descritto successivamente) ma è di stampo più pratico perché tralascia la parte di diffusione e trasmissione dell'importanza della security culture all'interno di un'organizzazione.

Il training è una delle basi più importanti per poter creare una cultura organizzativa. Per training non si intende esclusivamente la formazione iniziale che viene data ai nuovi dipendenti appena dopo l'assunzione, nella quale la sicurezza è un aspetto come tanti altri (e spesso consiste solo nella lettura e firma di un documento che contiene le politiche aziendali sulla sicurezza), ma un processo molto più ampio e continuativo.

In accordo con Benson (2005) *"sia i nuovi che i vecchi dipendenti necessitano di una formazione regolare non solo per capire la propria job description, ma anche per rimanere aggiornati con i valori culturali della propria organizzazione"*.

[22] Con status si fa riferimento alla mansione e alle responsabilità di competenza del dipendente

Un programma di formazione efficace anche in ottica security deve quindi prevedere delle riunioni periodiche e fornire sia un'educazione formale, che faccia comprendere i valori aziendali e le procedure di sicurezza, sia un training operativo che faccia capire al meglio come implementare le procedure di sicurezza. Sempre Benson (2005) aggiunge che *"per le organizzazioni che credono nella creazione di una cultura definita su un valore generale, come la sicurezza, la qualità, o la filosofia lean, il training formale deve essere affiancato al job training. Questa formazione ha l'obiettivo di educare i dipendenti sull'importanza di questi valori, e su come incorporarli nei comportamenti quotidiani all'interno dell'azienda".*

L'impatto di questa politica diminuisce le vulnerabilità dell'azienda in ottica di prevenzione di una disruption, ed ha anche effetti positivi sulla resilienza dell'organizzazione come rilevano Rice e Caniato (2003) che spiegano come l'educazione e il training siano elementi indispensabili per creare una cultura della resilienza in azienda.

Dello stesso avviso è Tsiakouri (2008) che afferma *"la formazione delle risorse umane, che è la base della cultura aziendale di un'organizzazione, è focalizzata primariamente sull'aumento dell'efficienza. In ogni caso, quando le risorse umane sono formate, diventano anche più resilienti"*.

Un altro meccanismo per incrementare la competenza dei dipendenti sulle tematiche di sicurezza è la costituzione di team di lavoro; la socializzazione informale è infatti un meccanismo che consente la trasmissione e l'arricchimento del bagaglio di competenze personali.

Il coinvolgimento di esperti esterni è invece il metodo da utilizzare quando all'interno dell'azienda mancano le possibilità o un'entità organizzativa in grado di poter svolgere in prima persona una formazione sulle tematiche di sicurezza. Gli esperti esterni possono anche essere utilizzati per organizzare test pratici e verificare le capacità e le vulnerabilità dell'azienda.

Consapevolezza interna sulla sicurezza

Questo strumento si pone come obiettivo quello di diffondere e trasmettere a tutti i membri dell'organizzazione l'importanza della security culture. Questo implica un processo con impatti a livello di organigramma, di sistema di controllo e incentivazione dei dipendenti e di comunicazione interna.

È importante che in azienda venga stabilita un'entità responsabile della diffusione e trasmissione della security culture. A seconda della grandezza e della struttura dell'azienda questa entità può passare da un'unica persona (la cui mansione può anche non essere esclusivamente quella di responsabile della security) ad una funzione organizzativa sotto il controllo di un Chief Security Officer (CSO). Per la diffusione di principi e standard a tutti i livelli dell'organizzazione è importante che il responsabile della security sia legittimato dai dipendenti; per ottenere la legittimazione deve avere caratteristiche di leadership, che secondo l'accezione di Barrow (1977) è *"quel processo comportamentale che riesce ad influenzare gli individui o i gruppi e spingerli verso obiettivi fissati"*.

Per la funzione aziendale è invece più importante la legittimazione ricevuta dal livello manageriale d'azienda, che si riflette nella collocazione strategica nell'organigramma.

La comunicazione interna è il canale con il quale operativamente è possibile far aumentare la consapevolezza dei dipendenti. I metodi utilizzati possono essere differenti: si passa da volantini a giornalini periodici, a riunioni nelle quali si affrontano i temi riguardanti la security, allo sfruttamento del canale intranet aziendale o ad iniziative che promuovano la socializzazione informale (eventi d'incontro tra dipendenti e responsabili della security anche fuori dall'ambiente lavorativo). Il fattore che rende meno efficace una campagna di comunicazione, indipendentemente dal metodo utilizzato, è la mancanza di progettazione che fa si che la promozione della campagna stessa sia lasciata alla soggettività del momento e della persona responsabile. Come evidenzia Lacey (2009) "*le attuali campagne di consapevolezza falliscono perché sono costruite sugli sforzi individuali dei manager, piuttosto che sui principi della psicologia e della comunicazione. […] Infatti, è raro assistere a una campagna di consapevolezza sulla sicurezza che sia realmente basata sull'accertamento dei fatti, sulla ricerca e su principi scientifici. Modificare il modo di operare delle persone in un ambiente di lavoro non è così difficile come la maggior parte delle persone immagino, ma richiede una buona comprensione del comportamento umano e l'utilizzo di pratiche di comunicazione tipiche del marketing. I programmi di cambiamento devono basarsi su una strategia chiara, una buona comprensione delle aree chiave, un'analisi delle cause degli incidenti, e una serie coerente di interventi di recupero*".

È chiaro quindi come la comunicazione e l'istituzione di un'entità organizzativa responsabile della security non siano sufficienti ad ottenere quella che Benson (2005) definisce una "responsabilizzazione dell'azienda". "*Per far si che i valori culturali*

penetrino l'organizzazione, tutti i membri si devono sentire responsabili del loro sostegno. Se un dipendente non ritiene che la difesa dei valori culturali dell'azienda possa influenzare il suo lavoro non si sente obbligato a fare nulla. [...] Il livello di responsabilità deve essere chiaramente legato a degli incentivi (o disincentivi) per determinati comportamenti".

Questa responsabilizzazione è quindi possibile ottenerla con la progettazione di un sistema di incentivazione e feedback sulla sicurezza. Tutti i sistemi di questo tipo devono partire dall'assegnazione di responsabilità e obiettivi di sicurezza ai dipendenti e procedere con lo sviluppo di un sistema di misurazione chiaro e con metriche precise. Sempre Benson (2005) aggiunge che *"senza un solido sistema di misurazione, i dipendenti si possono sentire persi nello svolgimento delle proprie mansioni. Questo perché i dipendenti percepiscono che il management non pone l'accento sull'allineamento delle prestazioni di lavoro con i valori culturali promossi".*

Esistono due differenti tipologie di sistemi di misura; da un lato è possibile effettuare un'analisi di tipo finanziaria, associando gli investimenti effettuati in politiche di security a risultati quantificabili economicamente, come riduzione di perdite potenziali oppure ore di lavoro guadagnate per la diminuzione di ispezioni. Questa metodologia è utile per allineare la politica sulla security agli obiettivi aziendali di alto livello. L'altra metodologia prevede di fare dei controlli interni per verificare la corretta implementazione delle pratiche di sicurezza. Le squadre che effettuano il controllo possono essere esterne o interne, e spesso le aziende utilizzano team già impiegati per il controllo di qualità o di sicurezza sul lavoro, istruendoli per la verifica degli standard di security.

L'ultimo aspetto per rendere il sistema di sicurezza efficace è il rilascio di feedback costanti al personale. *"Tenere i dipendenti informati sui processi di verifica e sui loro risultati rafforza l'impatto della sicurezza sul loro benessere e su quello della società"* (Benson, 2005)

Per rendere il sistema maggiormente efficace è possibile associarlo ad incentivi e punizioni anche se il rischio di turbare la gestione delle risorse umane è decisamente maggiore (soprattutto nei casi in cui la misurazione, le metriche e gli obiettivi sono ambigui). Incentivi e punizioni non è detto che siano sempre di natura economica: per

esempio il sistema "penalty box"[23] sposta a mansioni meno desiderabili quei dipendenti che non hanno rispettato le politiche e gli standard di sicurezza imposti.

Aspetti soft

Fanno parte di questo strumento i valori condivisi all'interno dell'organizzazione che creano una cultura organizzativa e che riescono ad influenzare le pratiche di lavoro quotidiano. In termini generali Lau e Ngo (1996) hanno concettualizzato la cultura organizzativa come un modo di intendere comune e sentimenti condivisi dai membri di un'organizzazione; fanno parte di questa condivisione filosofie, ideologie, valori, aspettative, assunzioni, percezioni, norme, comportamenti, tradizioni e miti.

Sulla stessa linea di pensiero Bonazzi (2002) evidenzia come *"gli approcci morbidi privilegiano gli aspetti culturali, simbolici, riflessivi ed i processi di conferimento di senso che i soggetti mettono in atto interagendo con le organizzazioni. Questi approcci, che sono fioriti nella seconda metà degli anni settanta si devono al fatto che le organizzazioni sono col tempo passate, dall'insoddisfazione derivante dagli approcci hard, a strumenti di controllo più raffinati, di natura normativa, basati sull'interiorizzazione da parte dei dipendenti di norme e valori"*.

Gli aspetti soft con specifico richiamo alla sicurezza sono quindi una modalità che l'azienda ha per diffondere i principi della security culture nell'organizzazione, creando una cultura organizzativa della sicurezza tra i propri dipendenti.

Questi strumenti agiscono in prima istanza sulla motivazione e sull'impegno dei dipendenti nel lavoro quotidiano. Le pratiche concrete per la diffusione di una cultura organizzativa della sicurezza partono dalla definizione di una mission e di un motto aziendale con specifico richiamo alla sicurezza; i valori espressi da queste iniziative devono essere una "*chiara e concisa manifestazione dei valori che l'azienda vuole utilizzare per fornire motivazione o aiuto nel processo decisionale"* (Benson, 2005).

Per far si che i valori espressi si diffondano a tutti i livelli organizzativi è necessario che la forma sia seguita dalla sostanza delle scelte strategiche aziendali e che vi sia un costante richiamo di questi valori in tutte le forme di comunicazione dell'azienda ai propri dipendenti (riunioni periodiche, giornalino aziendale, pubblicità, sito aziendale).

Altre pratiche più formali che permettono l'allineamento dei valori aziendali con quelli dei propri dipendenti sono l'istituzione di un codice etico o codice di condotta che

[23] Utilizzato dal gruppo IBM

rendano espliciti i comportamenti e i valori che l'azienda si aspetta dai propri dipendenti.

Risk management

Tabella 36: Risk management

APPROCCIO	STRUMENTO	
RISK MANAGEMENT	Business continuity planning	training dipendenti
		empowerment dei dipendenti
		piani d'azione
	Segnalare incidenti e debolezze	analisi della natura e delle cause degli incidenti (anche minori)
		"Swiss Cheese" model
		monitoraggio dei "near misses"
	Valutazione della conformità di sicurezza	strumenti preventivi di sicurezza basati sull'esperienza reale
		certificazioni

Gli strumenti inclusi nell'approccio di risk management, fanno parte di un insieme di strumenti più amplio e diversificato che fa riferimento alle tecniche di gestione del rischio aziendale a 360 gradi. Tra questi abbiamo selezionato gli strumenti coerenti con il nostro ambito di ricerca, ovvero strumenti di stampo culturale utili per lo sviluppo di una security culture. Autry e Bobbitt (2008) hanno incluso questa tipologia di strumenti nella famiglia "Security preparation and planning" nell'ottica di aumentare la supply chain security orientation di un'azienda.

Fanno parte di questa categoria tre famiglie di strumenti.

Business continuity planning

Le iniziative di business continuity planning sono orientate a descrivere il modo in cui un'organizzazione può far tornare operative le sue funzioni critiche entro un predeterminato periodo di tempo, a seguito di una disruption. Il BCP costituisce lo strumento attraverso cui un'organizzazione si prepara per futuri incidenti che possono minacciare le sue funzioni vitali e la sua sopravvivenza a lungo termine. Secondo Zsidisin et al. (2005) un BCP deve essere costituito da 4 fasi: creazione di consapevolezza, prevenzione (riduzione probabilità accadimento), piano di rimedio (aumento resilienza) e gestione della conoscenza. Queste fasi sono necessarie alle aziende che vogliono proteggere se stesse e le proprie supply chain da rischi esterni.

Dal punto di vista della security culture, gli strumenti più significativi per l'implementazione di un BCP sono le azioni rivolte alla responsabilizzazione e formazione dei dipendenti o la stesura di piani d'azioni formali da seguire al verificarsi di una disruption. Questo tipo di iniziative raggiungono il medesimo obiettivo con due filosofie diverse. Le iniziative di training (descritte precedentemente nella famiglia "Competenza dei dipendenti sulle tematiche di sicurezza") specifico per la gestione delle minacce, devono essere affiancate ad un processo di empowerment dei dipendenti che secondo Autry e Bobbitt (2008) è un fattore critico per la messa in sicurezza della supply chain. Gli autori ritengono infatti che la responsabilizzazione dei dipendenti sia indispensabile per affrontare o gestire minacce nella supply chain direttamente, senza dover chiedere il permesso ai superiori o dover consultare la policy aziendale.

I piani d'azione sostengono al contrario un'altra filosofia di pensiero che vuole una formalizzazione preventiva dei comportamenti e dei processi da mettere in atto una volta verificatasi una disruption, rispetto alla totalità delle funzioni aziendali: persone, processi, attrezzature, tecnologie IT etc. Sempre Autry e Bobbitt (2008), tramite uno studio sul campo, spiegano come la formalizzazione delle procedure (messe per iscritto e divulgate) è di notevole aiuto nell'affrontare situazioni impreviste di vulnerabilità o disruption. Per esempio la sola formalizzazione dei ruoli e delle responsabilità che ogni dipendente deve avere in caso di situazioni impreviste, velocizza il ripristino dei normali processi di business. Dall'analisi di queste due alternative, è possibile concludere che un approccio strutturato alle iniziative di BCP può comprendere entrambe le tipologie di strumenti, migliorando la resilienza totale d'azienda.

Segnalare incidenti e debolezze

In un programma per la gestione dei rischi con un'ottica di miglioramento continuo sulla base delle vulnerabilità d'azienda, è necessaria un'attenzione particolare alla segnalazione di incidenti e debolezze. Questo strumento comprende diversi processi che possono essere riassunti nell'analisi della natura e delle cause degli incidenti, nell'incorporazione di controlli su più livelli ("Swiss cheese model") e nel monitoraggio dei near misses.

Lacey (2009) ha condotto uno studio su questo tipo di strumento confrontando i "safety incidents" con i "security incidents"; il risultato è che la maggior parte degli incidenti sono senza colpe specifiche e non possono essere direttamente attribuibili a qualche individuo. In particolare *"i security incident sono il risultato di una combinazione di*

fattori piuttosto che dell'azione di un singolo individuo. In questi casi individuare un capro espiatorio è solamente una cortina fumogena che devia dalle azioni necessarie per l'analisi dei fattori che hanno causato l'incidente". L'autore per questi motivi ritiene che l'approccio tradizionale, basato sulla paura di punizioni ai danni dei dipendenti, non sia produttivo e al contrario faccia sviluppare una cultura in azienda che impedisca il corretto report e studio delle cause reali di un incidente. Una corretta security culture, invece, deve prevedere una consapevolezza basata sulle informazioni dei rischi di sicurezza, ovvero: *"la volontà di denunciare debolezze o punti deboli, la franchezza nelle valutazioni di conformità della sicurezza e un grado di empowerment che consenta al personale di adottare misure correttive".*

Sempre lo stesso autore in un libro pubblicato nel 2009 rileva come la maggior parte degli errori che producono security incident sono causati da fattori umani non associabili a cattivi comportamenti (Lacey, 2009); *"fattori come stress, mancanza di training o supervisione e sistemi mal progettati sono spesso la causa degli attuali buchi di sicurezza. Il management non dovrebbe quindi punire gli individui per gli errori commessi e le loro omissioni senza prima investigare sulle ragioni dei loro errori. La risposta logica ad una mancanza di sicurezza è da ricercate nell'analisi di cosa è andato storto piuttosto che sull'attribuzione della colpa".*

Per un programma di risk management è quindi indispensabile che vengano condotte delle analisi sulla natura degli incidenti, per comprendere le ragioni che li hanno causati. Quest'analisi dei rischi non deve avere lo scopo di prevedere futuri incidenti ma deve mappare i fattori alla base di quest'ultimi, per poter progettare delle azioni mirate di miglioramento.

Sempre David Lacey (2009) afferma come oltre all'analisi della tipologia di rischi debba essere implementato un approccio sul modello "Swiss cheese" che mira a prevenire collettivamente un incidente incorporando controlli su più livelli aziendali. Questo modello, già implementato per i programmi di safety da diversi anni, fatica ad essere applicato anche per quelli di security. Il modello pone particolare enfasi sul monitoraggio dei "near misses", ovvero su quelle situazioni di potenziale pericolo che non si sono tradotte in incidenti. A questo proposito uno studio sulle cause dei safety incident già nel 1932 rivelava come per ogni incidente maggiore (nel quale qualcuno muore o rimane seriamente infortunato) ci sono una media di 29 incidenti minori nei quali qualcuno si infortuna lievemente, e quasi 300 near misses (Heinrich, 1932). Lo

stesso ragionamento vale anche per i security incident, sottolineando l'importanza di questo strumento per la prevenzione di un incidente di grossa portata.

Valutazione della conformità di sicurezza

Questo strumento è strettamente legato alla segnalazione di incidenti e debolezze ma mentre il primo è più incentrato sulla individuazione delle vulnerabilità, quest'ultimo pone maggiore enfasi sul controllo della conformità rispetto requisiti di sicurezza.

La valutazione di conformità può essere eseguita sia internamente all'azienda, sia nella supply chain con ispezioni e controlli effettuati dall'azienda stessa in prima persona o da un ente terzo. Il livello base della valutazione prevede l'allineamento dell'azienda rispetto a determinate procedure di sicurezza, generalmente riconducibili agli standard progettati dai principali programmi di sicurezza obbligatori o volontari (paragrafo 3.1). In ottica di un pieno sviluppo di una security culture, oltre alle certificazioni, è necessario verificare se sono presenti degli strumenti di valutazione preventiva della sicurezza basati sull'esperienza di passati incidenti. Come rileva Lacey (2009) *"i security manager mettono meno enfasi, rispetto alle proprie controparti che si occupano di safety, nell'incorporazione di misure di sicurezza preventiva quando progettano un nuovo sistema o un nuovo processo. E quando lo fanno, con più probabilità si basano sulla valutazione di rischi teorici piuttosto che prendere spunto dagli incidenti che si sono verificati nella vita reale dell'azienda".*

Total quality management

Tabella 37: Total quality management

APPROCCIO	STRUMENTO	
TOTAL QUALITY MANAGEMENT	Partnership	norme di cooperazione
		relazioni di lungo termine
		condivisione di rischi, premi e responsabilità
		sviluppo della fiducia
	Collaborazione tra dipendenti	condivisione di rischi, premi e responsabilità
		teamwork
	Forza lavoro multidisciplinare	interazione cross-funzionale
		assunzione di persone con specifiche competenze
		training dei dipendenti
	Continuous improvement	funzione/posizione dedicata alla security (CSO)
		supporto del top management
		controllo dei processi esistenti
		empowerment dei dipendenti

Focus sul cliente	-
Knowledge management	apprendimento inter-aziendale
	istituzionalizzazione della conoscenza

Il Total Quality Management è un approccio integrato, composto da pratiche e valori, il cui obiettivo è di migliorare la qualità dei prodotti e servizi di un'azienda tramite la scelta della modalità più competitiva di soddisfazione continua dei bisogni dei consumatori (Gunasekaran e McGaughey, 2003).

Coerentemente al nostro ambito di ricerca, abbiamo selezionato gli strumenti riconducibili ad un approccio di TQM che, in ottica di supply chain, siano importanti per lo sviluppo di una security culture. Questi strumenti sono stati classificati da diversi autori come gli elementi "soft" del TQM; riprendendo la suddivisione delle pratiche di TQM di Zairi e Baidoun (2003) gli strumenti soft comprendono tutti quei valori come la leadership, il coinvolgimento dei dipendenti, e le politiche di qualità di lungo periodo che per loro stessa natura sono difficilmente misurabili. Questi fattori impattano sulla massimizzazione del supporto a tutti i livelli dell'organizzazione e del coinvolgimento dei dipendenti negli obiettivi di qualità dell'organizzazione. Secondo gli autori c'è una buona possibilità che il processo di TQM fallisca se non viene posta sufficiente attenzione su questi fattori "soft". Al contrario, i fattori "hard" includono tutte le pratiche e le politiche misurabili del TQM, alla base del processo di miglioramento continuo e direttamente riconducibili alle operations aziendali.

Partnership

Assumendo un'ottica di supply chain, le relazioni di lungo periodo all'interno della filiera sono indispensabili sotto i punti di vista della qualità, dell'affidabilità e della sicurezza; agiscono quindi sulla totalità delle prestazioni collegabili al SCM. Entrando nel dettaglio della partnership, le norme di cooperazione tra partner di filiera consentono una *"percezione dello sforzo comune dei partner per raggiungere obiettivi individuali e comuni con successo, senza utilizzare azioni opportunistiche"* (Siguaw et al., 1998). Le norme di cooperazione sono quindi necessarie per esplicitare i requisiti della collaborazione tra i partner, essendo presente la necessità di combinare sforzi comuni e dovendo cooperare con diversi attori nella filiera. Lo sviluppo della fiducia reciproca è indispensabile per sostenere una relazione di lungo periodo. La fiducia, definita da Morgan e Hunt (1994) come la sicurezza nell'integrità e nell'affidabilità del partner, è il valore culturale più importante per l'instaurazione di una relazione collaborativa, e si

traduce in un trasferimento di informazioni e conoscenze e nella condivisione di obiettivi comuni, fornendo un grosso aiuto nel superamento delle difficoltà inter-organizzative.

Il commitment, sempre secondo Morgan e Hunt (1994), è il secondo valore culturale più importante, ed è visto come un impegno continuativo verso il partner per mantenere il massimo sforzo nella relazione di collaborazione esistente.

Questi valori si consolidano nel tempo in una relazione di partnership, come evidenziato da Min et al. (2004): *"le aziende che si dimostrano meritevoli di fiducia sono disposte a condividere rischi, premi e informazioni con altre aziende nella filiera. Quando il commitment è incoraggiato da un'azienda, questa sarà propensa a cooperare con altre aziende per implementare una gestione condivisa della supply chain. […] Quando un'azienda collabora con altre organizzazioni ad essa compatibile* (che presenta lo stesso commitment e si dimostra meritevole di fiducia), *ci saranno effetti positivi sulle relazioni tra tutte queste. In aggiunta, le aziende con un forte supporto manageriale al SCM avranno leadership e commitment per proporre i cambiamenti necessari all'interno della supply chain".*

Collaborazione tra dipendenti

La collaborazione orizzontale è stata menzionata da molti autori che hanno approfondito tematiche legate alle pratiche di TQM ed il suo effetto finale si riscontra nell'aumento della qualità del lavoro quotidiano. Con il termine qualità possono essere comprese differenti prestazioni, ma noi ci concentreremo su quello che riguarda l'impatto di questo strumento sulla security d'azienda.

Sia negli studi sul TQM che in quelli relativi alla sicurezza della supply chain, il team è stato individuato come un meccanismo importante per aumentare sia la sicurezza preventiva che la resilienza; l'obiettivo è quello di lavorare insieme per trovare una soluzione migliore e condividere le responsabilità. Già Schein (1992) evidenziò l'importanza del lavoro in team, in riferimento al livello di cultura "assunti di base": "*la performance del team è più importante della performance individuale".* Dean e Bowen (1994) hanno ritenuto il lavoro in team una forma indispensabile di collaborazione tra dipendenti nelle pratiche di gestione della qualità; *"l'identificazione delle esigenze di tutti i membri del gruppo di lavoro nel processo decisionale, il lavoro per trovare una soluzione comune e la condivisione di responsabilità spingono i dipendenti di una funzione a lavorare a stretto contatto in un team per risolvere i problemi esistenti".*

Altri autori come Black e Porter (1996) e Ueno (2008) hanno classificato il lavoro in team come una delle pratiche predominanti nella promozione di un servizio di qualità.
Un'azienda per diffondere la cultura del lavoro in team può agire su più livelli: da una parte è importante la comunicazione interna fin dalla formazione iniziale che deve trasmettere l'importanza del lavoro di squadra, dall'altra legare una forma di incentivazione al team e non al singolo individuo è un differente tipo di meccanismo che permette all'azienda di dimostrare a tutti i dipendenti il suo supporto.

Forza lavoro multidisciplinare

Avere una forza lavoro multidisciplinare è necessario per aumentare la flessibilità delle risorse umane con diretto impatto sull'aumento della resilienza aziendale.
Come rilevano Wu et al. (2011) le pratiche esplorative[24] richiedono interazioni cross-funzionali e cooperazione. Esponendo i dipendenti a differenti prospettive, che derivano da altre aree funzionali, questi avranno maggiori possibilità di trovare soluzioni innovative.
Il training cross-funzionale è il mezzo con il quale si aumenta il bagaglio di esperienza dei dipendenti. *"Nella formazione esplorativa si enfatizza il training multidisciplinare così che i dipendenti possano attivamente insegnare e imparare dagli altri, generando pensiero creativo e la ricerca di nuove soluzioni".*(Wu et al., 2011)
Caniato e Rice (2003) hanno individuato la forza lavoro multidisciplinare come una pratica per aumentare la flessibilità di un'azienda, e quindi per poter rispondere più efficacemente ad una disruption. La flessibilità della forza lavoro è necessaria perché permette all'azienda di utilizzare della capacità presente in un'area aziendale per compensare lacune presenti in un'altra area. Gli autori, infatti, nella classificazione delle risposte ad una disruption mediante strumenti di resilienza, evidenziano come i vantaggi nell'avere una forza lavoro multidisciplinare siano di poter spostare i dipendenti e la produzione se necessario. Gli svantaggi sono invece i costi da sostenere per il training multidisciplinare e per la modifica dell'organizzazione del lavoro.
Sempre Caniato e Rice (2003) nelle "Proactive initiatives" per la classificazione delle risposte ad una disruption, individuano nell'aggiunta di nuove competenze al capitale umano d'azienda uno strumento efficace. Queste figure in ottica di assunzione, devono

[24] Gli autori chiamano "training for exploration" quelle pratiche di apprendimento che sperimentano nuove vie e possibilità di apprendimento. Si contrappongono alle "training for exploitation" che sfruttano pratiche vecchie e consolidate nel tempo

avere un background e delle esperienze specifiche in ambito sicurezza (per esempio gli autori si riferiscono a ex-militari, ex-agenti di polizia etc.); integrando nel proprio network questa tipologie di figura professionale, secondo gli autori, le organizzazioni riescono ad avere un impatto positivo sull'aumento della propria resilienza.

Focus sul cliente

Il focus sul cliente è una pratica strettamente collegata all'implementazione di una politica TQM; infatti in letteratura questo strumento viene citato da tutti gli autori che spiegano come gestire una programma di TQM. Lo strumento è anche associato ai programmi di SCM come sottolineato da Talib et al. (2011) *"il top-management commitment e il focus sul cliente sono le pratiche più citate nelle strategie di TQM e SCM. […] Il focus sul cliente nel TQM include soddisfazione del cliente, gestione dei reclami, stretta partnership e altre pratiche simili che si possono trovare anche nelle pratiche di SCM".*

Wu et al. (2011) ribadiscono come il focus sul cliente rifletta uno dei principi fondamentali della gestione della qualità: il cliente è il giudice ultimo della performance di qualità.

Lo strumento, considerato in una sua accezione, si adatta particolarmente al trasporto intermodale per la caratteristica struttura della filiera; essendo infatti la supply chain composta da tanti attori di diversa estrazione, il focus sul cliente può essere inteso come una modalità di lavoro e di progettazione dei processi che vadano a soddisfare il cliente finale (industriale) di tutta la filiera. Si tratta quindi di indirizzare tutti gli attori della filiera ad abbandonare una modalità di lavoro individualista e ragionare con l'ottica comune riferita alla soddisfazione del cliente finale. Questo è molto più semplice per quegli attorti che sono a diretto contatto con il cliente industriale (MTO), mentre è molto più arduo per quegli attori, come i trazionisti ferroviari o gli operatori terminalistici, che spesso conoscono a malapena chi è il destinatario ultimo dei container che processano. Lo strumento prevede che per soddisfare appieno il cliente finale, in termini di puntualità e sicurezza del trasporto, gli attori siano disposti a collaborare e a progettare un processo integrato di filiera. L'incentivazione è un metodo che consente di stimolare tutti gli attori della supply chain a lavorare in modo integrato; questi incentivi devono arrivare forzatamente o dal cliente finale o dal MTO i quali usufruiscono direttamente dei vantaggi derivanti da una filiera integrata.

L'incentivazione può essere di tipo economico o legata all'aumento dei volumi di trasporto da affidare agli attori facenti parte della filiera.

Continuous improvement

Il continuous improvement è un ulteriore elemento che contraddistingue tutti programmi di TQM. Come descritto da Wu et al. (2011) le pratiche di gestione della qualità hanno necessità di essere supportate da un sistema culturale di sostegno alla qualità che consiste in tre elementi principali: *"fare la cosa giusta al primo tentativo, lottare per ottenere un miglioramento continuo e soddisfare i bisogni dei clienti"*. Il continuous improvement rientra quindi nei valori base necessari allo sviluppo di una cultura organizzativa, individuati già da Schein (1992) come gli "underlying requirement".

Questo stesso concetto, emerso dalla letteratura e riferito alla gestione della qualità in genere, può essere specificatamente riferito alla messa in sicurezza della supply chain. Un programma di miglioramento continuo, per essere applicato in maniera efficace, deve prevedere uno stretto controllo dei processi di sicurezza esistenti, un forte supporto del top management (meglio se con una funzione che si occupa esclusivamente di security, strumento già descritto nella "consapevolezza interna sulla sicurezza"), e una forte collaborazione da parte del livello operativo, migliorabile con un programma di empowerment dei dipendenti (descritto precedentemente nello strumento "Business Continuity Planning").

Come detto da Wu et al. (2011) *"le pratiche tradizionali si focalizzano sull'incremento del controllo e della consistenza del processo esistente, mentre quelle innovative sottolineano i cambiamenti dell'attuale processo per permettere il miglioramento continuo"*.

Il miglioramento continuo delle pratiche di security parte quindi dal monitoraggio dei processi a livello basso, ed essendo gli operatori a stretto contatto con il processo, sono gli attori determinanti per rendere efficace lo strumento. Si tratta quindi di un programma che deve partire dal management aziendale ma che necessita di trovare a livello operativo una piena collaborazione, come sostenuto da Mello e Stank (2005). Lo sviluppo di questa collaborazione verticale, ottenibile con riconoscimenti di tipo economico o con un miglioramento dello status[25] degli operatori, è quindi necessaria e non può prescindere da un pieno supporto da parte del management aziendale. Min et

[25] Con status si fa riferimento alla mansione e alle responsabilità di competenza del dipendente

al. (2004) sottolineano infatti come il supporto del top management giochi un ruolo fondamentale nel definire la direzione di un'azienda, e la sua assenza può portare ad un sabotaggio dei valori fondamentali dell'organizzazione nel livello operativo.

Knowledge management

La gestione della conoscenza completa gli strumenti culturali riferibili ad un approccio di TQM. In ottica di security il processo di apprendimento è alla base di qualsiasi sforzo relativo all'implementazione di un processo sicuro, sia intra-aziendale che inter-aziendale. In letteratura un particolare focus viene riservato al processo di gestione della conoscenza all'interno di una supply chain (inter-aziendale). Per esempio Spekman et al. (2002) discute come la supply chain sia un veicolo di raccolta per informazioni e conoscenza, e di come l'apprendimento in un contesto inter-aziendale dipenda da fattori come lo stadio della relazione tra due aziende. Powell (1998) ha studiato invece da che fattori è composto l'apprendimento inter-aziendale e ha concluso che si tratta di un processo complesso e su più livelli comprendente: apprendimento da e con i partner sotto condizioni di incertezza; apprendimento dal comportamento dei partner; sviluppo di routines e norme che possano mitigare i rischi di opportunismo e apprendimento su come immagazzinare la conoscenza appresa da differenti progetti e funzioni.

Caniato e Rice (2003) hanno sottolineato un altro aspetto legato alla conoscenza, ovvero che le esperienze più importanti devono essere *"acquisite e documentate in una forma utile"*.

A questo proposito, per l'implementazione pratica dello strumento è possibile sfruttare sistemi per la codifica e la gestione delle esperienze, diffusi soprattutto nei settori human intensive, che hanno l'obiettivo di immagazzinare e rendere disponibile le informazioni a tutti i livelli aziendali. Come sostenuto da Tsang (1999) *"per elevare l'apprendimento dal livello di individuo a quello di un'organizzazione, la condivisione e l'istituzionalizzazione delle esperienze è essenziale. La condivisione di informazioni fra individui aiuta a migliorare la sola conoscenza tacita in loro possesso"*.

Strategic alliance program

Tabella 38: Strategic alliance program

APPROCCIO	STRUMENTO	
STRATEGIC ALLIANCE PROGRAM	Sviluppo della consapevolezza sulla sicurezza con i miei partner	apprendimento inter-aziendale
		contratti con specifici requisiti di sicurezza
		educazione dei partner
	Riduzione delle differenze di cultura tra azienda e partner	sviluppo della fiducia
		comunicazione esterna
		hibridal cultural interface (HCI)
		socializzazione informale
	Partnership	norme di cooperazione
		relazioni di lungo termine
		Condivisone dei rischi, premi e responsabilità
		sviluppo della fiducia

Assumendo un'ottica di supply chain, i programmi per creare delle alleanze strategiche sono indispensabili per assicurare qualità e sicurezza al cliente finale. È un approccio di tipo inter-aziendale finalizzato ad ottenere una piena integrazione tra le aziende e con gli enti governativi presenti nella filiera intermodale.

Sheffi (2001) descrive come avere solide relazioni con i partner di filiera e con le agenzie governative sia necessario per assicurarsi rispetto ai danni sugli asset e sui prodotti, che faciliti la continuità nella supply chain. Conclude infine che la collaborazione tra aziende, e la collaborazione tra settore pubblico e privato è necessaria per far si che le iniziative di security abbiano successo.

Fanno parte di questo approccio tre tipologie di strumenti.

Sviluppo della consapevolezza della sicurezza con i miei partner

Fanno parte di questo strumento i programmi finalizzati ad ottenere un partner di filiera conforme agli standard di sicurezza imposti dall'azienda focale[26]. Alla base di questo programma ci deve essere un processo di apprendimento inter-aziendale (descritto precedentemente nello strumento knowledge management) e uno sforzo da parte dell'azienda focale nell'educazione dei partner di filiera. Le varie forme e tipologie di training sono state precedentemente descritte nello strumento "competenza dei dipendenti sulle tematiche di sicurezza"; le stesse tipologie di formazione applicabili ai

[26] Azienda in posizione di leadership della supply chain

propri dipendenti è possibile quindi metterle in pratica anche per i partner della SC nell'ottica di uno sviluppo della consapevolezza nella filiera intermodale.

Una strada alternativa per ottenere il medesimo obiettivo e senza impegnarsi in prima persona nella formazione, è quella di aggiungere clausole specifiche di security nei contratti che legano l'azienda ai partner. Seppur l'azienda in questo modo perda il contatto diretto con il proprio partner, Benson (2005) evidenzia come molte organizzazioni negli ultimi anni abbiano scelto questa strada. *"Questo ha implicato una migliore comprensione da parte dei fornitori su quali fossero le aspettative di sicurezza. Per alcune aziende l'educazione dei fornitori può anche fermarsi a questo. Altre, maggiormente proattive, hanno compiuto un passo ulteriore* (impegnandosi nella trasmissione dei requisiti di security richiesti nell'azienda partner) *per assicurarsi che i propri fornitori capissero l'importanza della security culture nell'organizzazione".*

Riduzione delle differenze di cultura tra azienda e partner

Questo strumento è complementare al precedente ma mentre lo sviluppo della consapevolezza esterna è più incentrato sull'educazione dei partner e su meccanismi di training, la riduzione delle differenze di cultura agisce sugli aspetti soft delle aziende, favorendo la compatibilità e l'integrazione reciproca. Con il termine "adattamento culturale" non ci riferiamo esclusivamente a relazioni tra aziende di Paesi differenti, ma comprendiamo anche le interazioni tra aziende con diverse modalità di organizzazione del lavoro (sia a livello di cultura aziendale che a livello operativo). Queste differenze possono nascere da diverse tradizioni, da una differente un'impronta fornita dal management o dai fattori di contesto relativi alle due aziende. L'adattamento culturale, secondo la definizione di Lin e Germain (1999) è un processo riferito ad una relazione diadica, nella quale entrambi le parti cercano di adattarsi alla cultura altrui. Lin (2004) propone anche un modello a tre stadi per descrivere l'adattamento culturale: *"capire, adattarsi e imparare"*. Lo sviluppo della fiducia (definita precedentemente nello strumento partnership) reciproca è un elemento critico in questo tipo di relazioni, e studiosi come Mello e Stank (2005) hanno determinato che è necessaria per lo sviluppo di comportamenti di cooperazione, come flessibilità e collaborazione.

Jia e Rutherford (2010), sulla base del modello a tre stadi di Lin (2004), hanno cercato di schematizzare il processo di evoluzione di adattamento culturale (Figura 42). Nel primo stadio (stranger) le parti sono all'inizio del percorso di esplorazione reciproca, e si considerano ancora come stranieri. Nella seconda fase (acquaintance) la relazione si

espande e aumenta l'interdipendenza tra le parti e i benefici comuni. Nel terzo stadio (partner) la relazione è matura e realizza i vantaggi di una partnership strategica caratterizzata da fiducia e impegno. Parallelamente a questo modello gli autori rappresentano quella che definiscono la "hybrid cultural interface (HCI)" ovvero una *"cultura reciprocamente vantaggiosa che si crea all'interfaccia tra un cliente e un fornitore […] che è il risultato del processo di adattamento culturale che le parti hanno compiuto nella loro interfaccia".* .

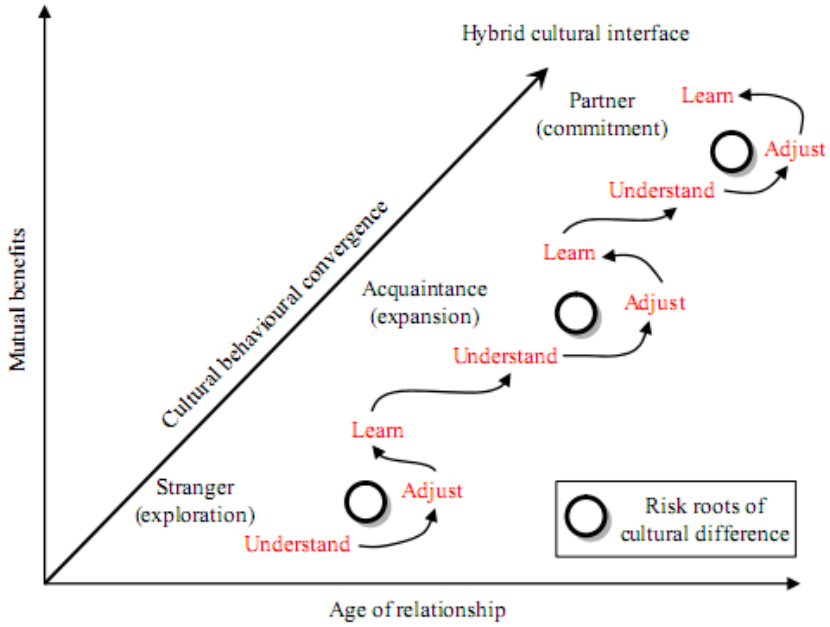


Figura 42: HCI

Lo sviluppo della HCI è possibile solamente se gli individui riescono a superare i perimetri della propria cultura; è evidente come lo sviluppo della fiducia e la socializzazione informale siano necessari per questo processo.

Operativamente un'azienda per poter realizzare una HCI con il partner, deve creare le condizioni per permettere alle due aziende di adattarsi reciprocamente; eventi informali come workshop, meeting e altre occasioni d'incontro sono le vie più praticate, per consentire al personale di entrare in contatto e poter creare una sintonia che trascende dal puro ambiente lavorativo. Tutto questo processo deve essere sostenuto da una chiara comunicazione esterna da parte delle aziende; come spiega Benson (2005) *"la comunicazione esterna può essere estremamente importante nell'affrontare i problemi della supply chain. Se un'azienda possiede particolari valori culturali che ritiene più importanti di altri, il partner ne deve essere informato per poter incorporare questi valori nei processi decisionali. […] Un'efficace comunicazione esterna è la chiave per*

assicurare che i valori culturali d'azienda siano supportati all'interno della supply chain".

Partnership

Questo strumento è stato precedentemente descritto nell'approccio di Total Quality Management.

4.3.3 Prestazioni di sicurezza

I Key Performance Indicator sono gli indicatori che consentono di monitorare la performance di sicurezza. Prima di procedere a una definizione dei KPI, è opportuno definire nel dettaglio la performance di sicurezza su cui gli strumenti culturali possono impattare.

Abbiamo visto nel paragrafo 2.3.4 che i benefici ottenibili dall'applicazione degli strumenti di Supply Chain Security, impattano su molteplici prestazioni aziendali, tra cui le principali sono efficienza, efficacia e trasparenza. Il nostro obiettivo è quello di valutare gli impatti che gli strumenti culturali individuati hanno sulla prestazione di sicurezza.

La prestazione di sicurezza, come evidenziato nel paragrafo 2.3.3, è il risultato di una minor vulnerabilità ottenibile dalla riduzione della probabilità di accadimento e della severità delle conseguenze di un evento di rischio, in accordo col framework della vulnerabilità di Sheffi e Rice (2005) illustrato in Figura 34.

In riferimento allo schema degli hazard/perils proposto da IMCOSEC illustrato in Figura 33, l'evento di rischio abbiamo visto essere la manifestazione di due possibili minacce:

- intenzionali (furti, manipolazione, contrabbando e attacchi terroristici),
- non intenzionali, di tipo naturale (eventi catastrofici) e "man-made" (errore umano, errore tecnologico),

Volendo proporre un'analisi che consideri la sicurezza nel suo più ampio spettro di accezioni – quindi in termini di sicurezza preventiva da minacce intenzionali e da minacce non intenzionali "man-made", e di sicurezza protettiva, definita resilienza, da ogni possibile minaccia –, al termine sicurezza attribuiamo due differenti significati:

1. *"Sicurezza da Attacchi"* atta a ridurre la probabilità di minacce intenzionali.
2. *"Sicurezza di Fornitura"* atta a ridurre la probabilità di minacce non intenzionali e le conseguenze di impatto della disruption causata da qualsiasi tipo di minaccia, così da garantire la continuità del business.

Tabella 39:Tipologie di sicurezza

	Sicurezza preventiva	**Resilienza**
Attacchi intenzionali	Sicurezza da attacchi	Sicurezza di fornitura
Attacchi non intenzionali		

Questa classificazione alternativa vuole quindi andare oltre il focus tradizionalmente considerato in letteratura (corrispondente alla nostra sicurezza da attacchi). Per la definizione della sicurezza di fornitura abbiamo tenuto conto che, in riferimento alla resilienza, non ha senso distinguere tra minacce di tipo intenzionale o non intenzionale (il focus è sull'effetto non sulla causa) mentre considerando attacchi di tipo non intenzionale (vedi errori umani) gli strumenti che ne riducono la probabilità di accadimento sono correlati a quelli per la riduzione delle conseguenze (vedi l'educazione/formazione degli operatori).
Per ogni tipologia di sicurezza abbiamo individuato i possibili KPI che spiegano la cattiva performance della prestazione finale.

Sicurezza da attacchi

Per la "Sicurezza da attacchi" sono stati individuati i seguenti KPI:

- **Furti:** *"non autorizzata rimozione di parte del contenuto del container o del container stesso. Il furto del carico può essere organizzato da un membro della filiera intermodale oppure da qualcuno connesso a loro che ha ottenuto informazioni privilegiate. In alcuni casi può essere organizzato da terze parti senza averlo pianificato in anticipo. Il furto dell'intero container può avvenire a seguito di una perlustrazione del container e un piano noto, oppure senza alcuna pianificazione"* (Daschkovska, 2010).
  La duplice valenza implica la possibilità di scomporre ulteriormente questo KPI. La metrica dei furti può essere espressa in pezzi, ILU o euro.
- **Manipolazione**: *"è un piazzamento non autorizzato di qualsiasi merce proibita (bombe, armi, droga, persone) in un container, effettuata da un membro del processo di trasporto, caricamento e scarico".* Può essere un membro interno o esterno al processo. La manipolazione può avvenire durante la fase di carico prima che il contenuto venga sigillato, oppure durante il trasporto dopo aver

chiuso e sigillato il contenitore. Nel caso di persone essa può essere usata per il trasporto illegale di clandestini o talvolta di terroristi, come è accaduto nel porto di Goia Tauro nel 2001 (paragrafo 2.4). Nella manipolazione rientra anche il contrabbando di armi, bombe, esplosivi, materiali chimici etc. Un caso particolare di manipolazione può portare allo scenario estremo del *"dirottamento della ILU"*, che avviene quando *"il container viene intercettato in qualche punto lungo la filiera, aperto illecitamente; vengono inserite armi a distruzione di massa nel carico, il container viene chiuso e sigillato di nuovo, per poi fare detonare l'ordigno nel punto desiderato"* (Crist et al., 2005). Il KPI viene espresso in numero di ILU manipolate.

Sicurezza di fornitura

Per la "Sicurezza di fornitura" sono stati individuati i seguenti KPI:

- **Ritardo di fornitura subito [1]:** causato dal fornitore di filiera, espresso in tempo;
- **Ritardo di fornitura causato [2]:** espresso in tempo;
- **Ritardo di fornitura al cliente finale:** causato da tutti gli attori della filiera, espresso in tempo;
- **Stock-out:** equivalente del ritardo ma espresso in pezzi o euro.

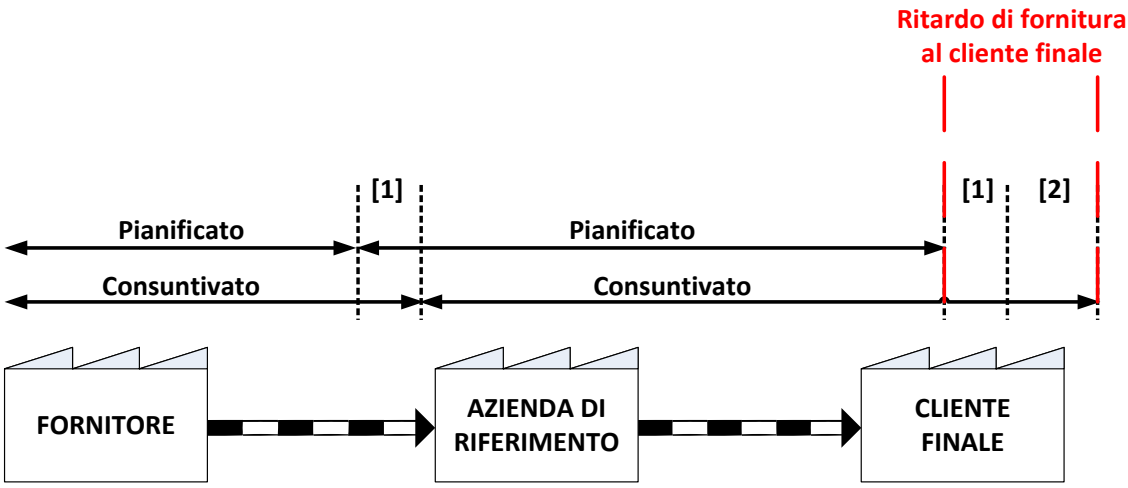


Figura 43: Sicurezza di fornitura

4.3.4 Fattori causa

La prestazione riassunta dal KPI è l'effetto del verificarsi di differenti fattori causa.
In altri termini, attraverso il fattore causa spieghiamo le relazioni di causa-effetto che collegano lo strumento al KPI. Ogni KPI, infatti, è il risultato di alcuni fattori che possono manifestarsi all'interno di un'organizzazione. Gli strumenti individuati possono impattare su una o molteplici cause che determinano il KPI.
Abbiamo visto nell'analisi della letteratura relativa alla cultura di sicurezza e fattore umano (paragrafo 4.1.3) che una disruption può essere causa di fattori umani, organizzativi o inter-organizzativi (Catino, 2002).
Prendendo spunto dalla teoria sulla natura degli incidenti sviluppata dallo stesso Catino, all'interno del nostro ambito di ricerca possiamo ricondurci ai seguenti fattori causa.
Tra i fattori di natura individuale rientrano: fenomeni collusivi tra persone interne o esterne all'organizzazione, sia che ricoprano posizioni a livello operativo sia d'ufficio; errori di qualsiasi natura nell'implementazione di procedure predefinite a livello del singolo individuo o di un team all'interno dell'organizzazione; non osservanza delle procedure da parte degli individui dell'organizzazione.
Tra i fattori di natura organizzativa rientrano gli errori imputabili a chi definisce le procedure e le politiche gestionali in fase di pianificazione: infatti un operatore potrebbe perseguire un obiettivo corretto, ma con un piano errato. In questo caso si parla di debolezze e errori *"organizzativamente costruiti"* (Catino, 2002).
Tra i fattori di natura inter-organizzativa troviamo tutti quegli errori che possono nascere dall'interazione con altre organizzazioni (fornitori o partner), ad esempio a causa dell'assenza di collaborazione e comunicazione tra le parti, di una limitata visibilità sul partner/fornitore ed infine dell'inadeguatezza del partner/fornitore dovuta a lacune presenti nelle sue procedure e politiche gestionali.
In definitiva associamo ai KPI di sicurezza da attacchi (furti e manipolazioni) i seguenti fattori causa:

- collusione;
- errata implementazione delle procedure;
- mancata implementazione delle misure esistenti;
- inadeguatezza delle procedure/politiche gestionali;

mentre ai KPI relativi alla sicurezza di fornitura (ritardi e stock out):

- mancata implementazione delle politiche gestionali;

- errata implementazione delle procedure gestionali;
- inadeguatezza politiche gestionali;
- mancata collaborazione/comunicazione con i partner;
- Non sufficiente visibilità/integrazione con i partner;
- inadeguatezza partner;

ad eccezione per il ritardo di fornitura che subisco a cui sono possibili associare solo i fattori causa relativi al mio partner.

4.4 Conclusioni

In questo capitolo abbiamo delineato 5 domande di ricerca sul possibile utilizzo e impatto degli strumetni di tipo culturale, che abbiamo visto appartenere ad un filone di ricerca poco sviluppato ma con una potenziale influenza sulla sicurezza di una ILU supply chain.

Abbiamo quindi formulato un modello teorico in risposta ipotizzando l'esistenza di caratteristiche peculiari delle aziende (fattori di contesto) che potessero spiegare i differenti utilizzi e i differenti impatti sulla sicurezza. In particolare ci riferiremo alla sicurezza da attacchi (probabilità di minacce intenzionali) e di fornitura (probabilità di minacce non intenzionali e conseguenze a disruption dovute sia a minacce intenzionali che non), per le quali abbiamo definito degli specifici KPI (furti/manipolazione e ritardo/stock-out) e dei fattori causa che determinano le prestazioni di sicurezza. Nel capitolo 5 definiremo la metodologia per condurre la ricerca sul campo.

5 Metodologia di ricerca

Il caso di studio è una strategia di ricerca finalizzata alla formazione, benché non necessariamente riconducibile ad un particolare tipo di evidenza empirica o metodo di raccolta dati (Yin, 2011).

Esso descrive l'evoluzione di un fenomeno e le sue interazioni con il contesto reale, proprio quando i confini tra fenomeno e contesto non sono chiaramente evidenti.

Un caso di studio può includere dati quantitativi, qualitativi ed elementi teorici e ha l'obiettivo di sviluppare una teoria capace di spiegare i dati raccolti. I risultati finali del caso di studio sono di tipo descrittivo, tramite i quali viene spiegato a parole ciò che è stato appreso dai ricercatori.

L'elemento fondamentale di questa tipologia di indagine è il "caso". Denominato tecnicamente "unità di analisi", esso rappresenta un sistema reale in cui le componenti non devono necessariamente funzionare bene, ma ha l'unico scopo di permettere e facilitare la comprensione del fenomeno. Il caso non rappresenta cioè il vero oggetto di analisi, ma a partire da questo si cerca di spiegare un fenomeno più ampio all'interno del quale il caso si colloca.

In funzione del numero di casi presi in esame e delle finalità della ricerca si contraddistinguono quattro differenti tipologie evidenziate in Tabella 40.

Tabella 40: classificazione studio di casi

		Numero di casi presi in esame	
		uguale a uno	**maggiore di uno**
Finalità dello studio	**esplorativo**	Caso singolo esplorativo	Caso multiplo esplorativo
	descrittivo	Caso singolo descrittivo	Caso multiplo descrittivo

Mentre la dimensione "numero di casi presi in esame" è auto-esplicativa, quella di "finalità dello studio" merita un approfondimento. Si definisce esplorativo uno studio che viene effettuato per chiarire aspetti chiave del disegno di ricerca, il quale sarà sviluppato successivamente. Si definisce invece descrittivo un caso analizzato successivamente allo sviluppo del disegno di ricerca e che risulta quindi più circoscritto all'oggetto di interesse e ne analizza gli aspetti in modo più approfondito: è proprio il

disegno di ricerca a stabilite l'oggetto di interesse e il relativo livello di approfondimento.

Oltre alla classificazione proposta da Yin, Stake (1995) afferma che esistono altre due tipologie di studio: intrinseco e strumentale. Il primo è uno studio che si focalizza sul caso reale, approfondendo tutti i sui aspetti, analizzando situazioni ed eventi unici ma particolarmente utili. Lo studio strumentale ha invece una funzione di conferma e verifica della capacità di una teoria pre-esistente di spiegare un determinato fenomeno. Nel nostro caso, il fenomeno è che i fattori di contesto possano influenzare l'utilizzo e l'impatto degli strumenti culturali, non specificando in che modo possano farlo; il nostro studio è quindi di tipo strumentale. Considerando invece la classificazione di Yin (2011) il nostro studio si colloca nella categoria "caso multiplo descrittivo", tramite il quale abbiamo esaminato i processi e gli strumenti applicati in modo ricorrente per situazioni simili tra loro.

Riteniamo utile suddividere il nostro caso di studio in tre fasi logiche sequenziali, che andremo ad approfondire nei paragrafi seguenti:

- individuazione dell'unità di analisi;
- creazione degli strumenti per l'osservazione sul campo;
- raccolta dei dati;

Una volta creata la base di dati procederemo all'analisi ed elaborazione dati nel Capitolo 6.

5.1 Individuazione dell'unità di analisi

Quest'attività si propone di scegliere l'unità fondamentale di analisi sulla quale saranno poi raccolte tutte le informazioni utili per rispondere ai quesiti formulati paragrafo 4.2. L'individuazione dell'unità di analisi è un'attività critica, in quanto è dalla corretta scelta di questa che ne deriva la bontà dei risultati della ricerca e quindi l'affidabilità delle risposte alle domande espresse in fase di formulazione del disegno di ricerca. L'unità di analisi può essere rappresentata da: un singolo individuo, un gruppo di soggetti, un processo, un'organizzazione o una combinazione di più unità.

Per il nostro scopo, abbiamo ritenuto opportuno intervistare diverse aziende facenti parte della filiera intermodale strada-ferrovia che fossero il più eterogenee possibili secondo i fattori di contesto citati nel paragrafo 4.3.1. L'unità di analisi sulla quale

abbiamo focalizzato i nostri sforzi di raccolta dati può essere genericamente definita attraverso i seguenti punti:

- **Ambito di studio:** singola azienda all'interno della filiera intermodale strada-ferrovia
- **Soggetti coinvolti:** Posizioni di Amministatore Delegato, Dirigente/Responsabile Operativo o Commerciale, in ogni caso persone con particolari responsabilità in ambito di sicurezza
- **Contesto dello studio:** esplicito riferimento a tutti i fattori di contesto discussi, con una forte attenzione a tutte le interconnessioni con i relativi partner (fornitori e clienti) di filiera, data la sua forte eterogeneità
- **Area geografica:** nord Italia (Lombardia e Piemonte) e Svizzera
- **Intervallo temporale:** maggio-ottobre 2011

In Tabella 41 è elencato il campione di aziende da noi intervistato.

Tabella 41: Campione di aziende intervistate classificate in base ai fattori di contesto

Aziende	Fattori di contesto					
	Dimensione	Ambito	Ruolo	Integrazione verticale	Tipologia di merce	Internazio-nalizzazione
AMBROGIO	grande	strada-ferrovia	MV+GO	alta	A	INT
BAS LOGISTICS	piccola	strada	MV	bassa	A+P	INT
EWALS INTERMODAL	grande	strada	M	bassa	A+P	INT
FERCAM	grande	strada	M	bassa	A+P	INT
HOYER GROUP	grande	strada	MV	bassa	P	INT
HUPAC	grande	ferrovia	GO	alta	A+P	INT
INTERPORTO RIVALTA SCRIVIA	grande	strada-ferrovia	M+G	alta	A+P	INT
MARENZANA	piccola	strada	MV	bassa	P	INT
MAGAZZINI DESIO BRIANZA	piccola	strada-ferrovia	M+G	alta	N	INT
SOGEMAR	grande	strada-ferrovia	MV+GO	alta	A+P	INT
TI.MO.	piccola	ferrovia	G	bassa	A+P	ITA
TERMINALI ITALIA	piccola	ferrovia	G	bassa	A+P	ITA
VOTG	grande	strada	M	alta	P	INT
LEGENDA:	M = MTO, MV = MTO e vettore stradale, G = gestore terminal, GO = gestore terminal e operatore commerciale, P = merce pericolosa, A = merce ad alta appetibilità, N = merce non pericolosa e poco appetibile					

Nella Tabella 41 è illustrata inoltre la classificazione delle aziende intervistate secondo i fattori di contesto. La spiegazione per ogni fattore causa è riportata di seguito.

Dimensione

In riferimento alla Tabella 43 dei parametri per la definizione della dimensione delle imprese secondo la Raccomandazione della Commissione Europea 6 maggio 2003, n. 2003/361/Ce, al fine di semplificare le nostre analisi abbiamo accorpato le classi "micro impresa", "piccola impresa" e "media impresa" in un'unica classe considerando infine solo due classi: "piccola impresa", con un numero di dipendenti fino a 249 e fatturato fino a 50 mln € , e "grande impresa". Nella scelta del numero di dipendenti e del fatturato da considerare nella valutazione della dimensione aziendale, abbiamo fatto riferimento, in ordine di priorità, alle seguenti fonti: intervista, sito aziendale e altri siti. Nel caso di aziende appartenenti a un gruppo, abbiamo considerato i valori della capogruppo, in quanto la maggior parte degli strumenti culturali vengono applicati a livello corporate e si riflettono sulle business unit.

Tabella 42: numero dipendenti e fonti dell'unità di analisi

Azienda	Dipendenti	Fatturato (mln €)	Fonte
AMBROGIO (*)	50 - 249 solo Ambrogio Trasporti	Ambrogio (gruppo): 80 (2009)	Altro sito
BAS LOGISTICS (*)	BAS Group: 210 (di cui il 10% occupato nel settore intermodale)	BAS Group: 29 (di cui il 10% dal settore intermodale)	Intervista
EWALS INTERMODAL (*)	Ewals Cargo Care: 1.600 Ewals Intermodal: 70	Ewals Cargo Care: 395 -	Sito aziendale Intervista
FERCAM	1.845	430	Sito aziendale
HOYER GROUP (*)	5.200	990	Intervista
HUPAC	401	365,4	Sito aziendale
INTERPORTO RIVALTA SCRIVIA	600 di cui 500 tramite cooperativa	52	Intervista
MARENZANA	90 circa di cui 70 autisti	13,5	Intervista
MAGAZZINI DESIO BRIANZA (**)	36	11 (2008)	Intervista Altro sito
SOGEMAR (*)	Contship: 2.500 Sogemar: 150	Oltre 300 56	Sito aziendale Intervista
TERMINALI ITALIA (***)	Gruppo Ferrovie Italiane dello Stato: 31.595 Terminali Italia: 202	Gruppo Ferrovie Italiane dello Stato: oltre 2 mld Terminali Italia: 16,5 (2009)	Sito aziendale
TIMO	4 interni e 4 esterni	0,4 (0,75 previsioni 2011)	Intervista
VOTG (*)	VTG Group: 1.000 circa VOTG: 107	VTG Group: 629,4 VOTG:144,5	Sito aziendale

(*) vengono considerate a livello di gruppo
(**) nel caso di MDB non facciamo riferimento al gruppo Lucefin S.p.A. perché si occupa di un business completamente diverso
(***) nel caso di Terminali Italia non viene preso come riferimento il gruppo Ferrovie Italiane dello Stato, in quanto dall'intervista è emersa una netta distanza dalla capogruppo, la quale esercita una bassa influenza sulla gestione del terminal

Ambito, ruolo e integrazione verticale

Per la determinazione dell'ambito, ruolo e integrazione facciamo riferimento alla Tabella 43

Tabella 43: ruoli dell'unità di analisi

COMPANY / ATTORE	MTO	Vettore stradale	Operatore commerciale	Gestore terminal	Trazionista	Gestore rete ferroviaria
AMBROGIO INTERMODAL	X	X	X	X		
BAS LOGISTICS	X	X				
EWALS	X					
FERCAM	X					
HOYER	X	X				
HUPAC			X	X	X	
INTERPORTO RIVALTA	X			X		
MARENZANA	X	X				
MDB MAGAZZINI DESIO E BRIANZA	X		CG	X	CG	
SOGEMAR	X	X	X	X	(*)	
TERMINALI ITALIA			CG	X	CG	CG
TIMO				X		
VOTG	X		CG		CG	

CG = capogruppo
(*) = nuova società controllata

Ruolo

Per semplificazione abbiamo associato ad ogni ruolo una sigla nel seguente modo:

- M: MTO;
- MV: MTO e Vettore stradale;
- G: Gestore terminal;
- GO: Gestore terminal e Operatore commerciale.

Ambito

Essendo l'ambito il fattore di contesto di alto livello del ruolo ricoperto dall'azienda nel trasporto intermodale, ricaveremo le classi dell'ambito a partire dai ruoli svolti.

- Strada: chi svolge il ruolo di MTO o MTO e vettore stradale;
- Ferrovia: chi svolge il ruolo di gestore del terminal o gestore del terminal e operatore commerciale;
- Strada/Ferrovia: chi svolge almeno un ruolo dell'ambito strada e ferrovia congiuntamente.

Per questa ragione nella nostra analisi, ambito e ruolo verranno considerati congiuntamente partendo dal livello più alto e, se necessario, andando a dettagliare l'analisi a livello atomico di singolo ruolo

Integrazione verticale

In relazione a questo fattore di contesto, il nostro campione di aziende è stato suddiviso in due classi:

- integrazione alta: chi a livello di azienda o gruppo svolge almeno un ruolo sia nell'ambito stradale che ferroviario, oppure per quello ferroviairo svolge anche il ruolo di trazionista (NB: Terminali Italia, nonostante abbia la capogruppo che effettua trazione, la consideriamo non integrata per le stesse considerazioni effettuate sulla dimensione);
- integrazione bassa: le restanti.

È da sottolineare come con integrazione alta non necessariamente si intenda la completa integrazione di tutta la filiera, ma è sufficiente per considerarla tale che esista una consistente e significativa agglomerazione di ruoli.

Tipologia di merce

È possibile osservare dalla Tabella 41 come le tipologie di merce pericolosa (P) e ad alta appetibilità (A) siano comuni a quasi tutte le aziende, mentre solo un'azienda non trasporta merci pericolose o appetibili (N). Ne consegue che il nostro campione non può essere analizzato in base alla tipologia di merce trasportata perché non è possibile costruire cluster di analisi sufficientemente ampi e distinti tra loro.

Internazionalizzazione

Dalla Tabella 41 emerge che solo 2 aziende su 13 sono presenti solo sul territorio italiano, indicate con ITA, mentre le restanti, indicate con INT, fanno parte di un gruppo internazionale o presentano filiali al di fuori dei confini italiani. Questi numeri non sono sufficienti per determinare due cluster significativi per le nostre analisi.

5.2 Creazione degli strumenti per l'osservazione sul campo

Dopo aver definito la tipologia del caso di studio (caso di studio multiplo descrittivo – strumentale) ed aver delimitato la nostra unità di analisi con la selezione dei fattori di contesto maggiormente significativi, di seguito vengono spiegate le modalità con cui

abbiamo deciso di raccogliere i dati necessari per rispondere alle domande di ricerca. La modalità scelta è stata quella dell'intervista personale finalizzata alla compilazione di un questionario. L'intervista è stata strutturata con un'introduzione iniziale per spiegare lo specifico contesto della nostra analisi (security) e la definizione delle prestazioni di sicurezza (differenza tra attacchi e fornitura) e dei relativi fattori causa. Successivamente abbiamo richiesto ai nostri interlocutori una breve introduzione sull'azienda e cosa intendessero con il termine "sicurezza"; questo per cercare un confronto con il nostro focus di ricerca e cercare di aiutare gli intervistati a rimanere allineati con i nostri obiettivi durante l'intervista. Quindi siamo passati all'analisi puntualmente degli strumenti proposti, fornendo inizialmente una descrizione (supportata da esempi concreti di applicazione) e chiedendo se venissero applicati o meno in azienda. Abbiano distinto tra un'applicazione formale dello strumento [f], che implica una modalità standard e definita di utilizzo, da una non formale [n.f.] che al contrario non è standardizzata, e dalla non applicazione [NO]. In caso lo strumento venisse applicato (in modo formale o non) abbiamo chiesto se quest'ultimo avesse un impatto sull'aumento della sicurezza di attacchi e fornitura, e se si, quale fattore causa peggiorava o migliorava[27]. In caso lo strumento non venisse applicato abbiamo chiesto quali fossero i motivi. Dopo aver passato in rassegna tutti gli strumenti proposti abbiamo chiesto di indicarci quali fossero i più importanti ai fini di migliorare la security aziendale. L'intervista è proseguita con un'analisi sui fattori causa, richiedendo per ogni KPI proposto (Furti/manipolazioni e ritardo) quali fossero allo stato attuale le cause principali. In particolare abbiamo richiesto un impatto percentuale dei fattori causa sul KPI ma in diversi casi i nostri interlocutori non sono stati in grado di rispondere e quindi, in queste situazioni, abbiamo richiesto semplicemente di indicarci un ordine di importanza relativo tra i fattori causa. Come ultima domanda abbiamo chiesto se l'azienda utilizzasse dei sistemi per misurare la security aziendale e, se si, quale metriche utilizzassero. Le loro risposte hanno confermato la nostra scelta dei KPI per la sicurezza di attacchi e di fornitura, che sono gli indicatori che utilizzano la quasi totalità del campione.

In tutta l'intervista la problematica maggiore è stata quella di mantenere sempre allineati i nostri interlocutori con il nostro ambito di ricerca; spesso infatti non è stato

[27] I KPI di riferimento esprimono una cattiva prestazione di sicurezza; quindi se l'impatto dell'applicazione dello strumento peggiora un fattore causa, peggiora anche il KPI ad esso associato e migliora la prestazione di sicurezza complessiva d'azienda.

facile concentrarsi sugli aspetti di security piuttosto che di safety, o far capire la differenza tra la sicurezza di fornitura (che presuppone l'accadimento di una disruption) piuttosto che di un ritardo al cliente finale causato da inefficienze nella quotidiana gestione del business. Anche per questo motivo è stato indispensabile scegliere la forma dell'intervista personale, che permette una maggiore comprensione delle motivazioni alla base delle scelte degli intervistati. Nell'Appendice C riportiamo i documenti di cui ci siamo serviti per far capire agli intervistati, nella fase di primo contatto, che tipo di intervista avremmo condotto e le linee guida che abbiamo seguito per discriminare tra l'utilizzo più o meno formale di uno strumento.

5.3 Raccolta dati

Dopo le prime interviste abbiamo riscontrato quali fossero le maggiori difficoltà dei nostri interlocutori nell'affrontare i temi proposti e, per migliorare la loro comprensione, abbiamo apportato qualche modifica allo schema d'intervista. Anzitutto, per quanto riguarda la sicurezza di fornitura, abbiamo preferito utilizzare un unico KPI rispetto a quelli descritti nel paragrafo 2.3.4 (Figura 43: Sicurezza di fornitura) per rendere più immediata la comprensione del questionario; la scelta è stata quella di stabilire il KPI "ritardo di fornitura al cliente finale" come l'unico rappresentativo della sicurezza di fornitura (KPI che comprende gli effetti degli altri due). Un altro accorgimento è stato quello di accorpare gli strumenti "competenza dei dipendenti sulle tematiche di sicurezza" e "consapevolezza interna sulla sicurezza"; infatti fin dalla prime intervistate è emerso come i due strumenti venissero implementati congiuntamente, e come non fosse possibile separarne gli effetti. Abbiamo chiamato lo strumento risultato dall'accorpamento "sviluppo della consapevolezza interna sulla sicurezza".
Di seguito viene riportata la tabella che sintetizza i risultati delle tredici interviste effettuate.

Tabella 44: tabella riassuntiva del totale delle aziende

							# aziende	11			13			
								SICUREZZA DA ATTACCHI			SICUREZZA DI FORNITURA			
			Impatto del fattore causa sul KPI					26%	38%	35%	19%	69%	6%	6%
			Lo strumento viene utilizzato in azienda?											
# aziende	Importanza strumento	Numero strumento	f.	n.f.	SI	NO		Collusione	Errata/mancata implementazione delle procedure	Inadeguatezza delle procedure	Mancata collaborazione/ visibilità con i partner	Inadeguatezza partner	Errata/mancata implementazione delle politiche gestionali	Inadeguatezza delle politiche gestionali
10	20%	1	60%	10%	70%	30%		-17%	100%	17%	0%	0%	100%	14%
	90%	2	70%	30%	100%	0%		25%	100%	13%	10%	0%	100%	10%
	40%	3	60%	20%	80%	20%		86%	71%	0%	0%	0%	75%	0%
	50%	4	80%	10%	90%	10%		0%	100%	14%	0%	0%	89%	22%
13	0%	5	62%	15%	77%	23%		78%	89%	22%	10%	0%	70%	20%
	31%	6	31%	54%	85%	15%		0%	56%	100%	0%	18%	55%	100%
	0%	7	23%	0%	23%	77%		0%	0%	33%	0%	33%	33%	67%
	69%	8	46%	54%	100%	0%		9%	64%	91%	8%	31%	69%	92%
	8%	9	8%	23%	31%	69%		0%	50%	75%	50%	50%	50%	75%
	38%	10	77%	23%	100%	0%		36%	55%	82%	8%	62%	69%	85%
12	17%	11	100%	0%	100%	0%		80%	60%	80%	92%	67%	75%	67%
13	23%	12	54%	23%	77%	23%		25%	63%	38%	0%	70%	70%	40%
	0%	13	46%	15%	62%	38%		50%	50%	33%	38%	50%	50%	38%
	8%	14	0%	31%	31%	69%		-25%	25%	25%	75%	0%	50%	50%

Legenda strumenti:

(1) forza lavoro multidisciplinare, (2) collaborazione tra dipendenti, (3) integrità/lealtà dei dipendenti, (4) sviluppo della consapevolezza interna sulla sicurezza, (5) aspetti soft, (6) continuous improvement, (7) business continuity planning, (8) segnalare incidenti e debolezze, (9) knowledge management, (10) valutazione della conformità di sicurezza, (11) partnership, (12) sviluppo della consapevolezza sulla sicurezza con i miei partner, (13) riduzione della differenza di cultura tra azienda e partner, (14) focus sul cliente.

Nella Tabella 44 la prima colonna [# aziende] riporta il numero di aziende che hanno la possibilità di implementare lo strumento e che verranno quindi comprese nelle analisi numeriche. Tre aziende non hanno la possibilità di utilizzare gli strumenti 1,2,3,4 perché non possiedono del personale operativo dipendente (sono aziende di tipo M) mentre TI.M.O., considerati i pochi anni di vita, non ha avuto la possibilità di poter costruire veri e propri rapporti di partnership. La prima riga [# aziende] riporta il numero di aziende per cui ha senso considerare la sicurezza da attacchi e di fornitura; per due aziende (MDB e Marenzana), infatti, il problema della sicurezza da attacchi intenzionali non si pone neanche perché, gestendo esclusivamente merce industriale pesante o particolari materiali ADR, furti o manipolazioni non si sono mai verificati e non ci sono concrete possibilità che nel futuro si possano verificare[28]. La percentuale d'importanza dello strumento è stata determinata in base al numero di aziende che hanno individuato lo strumento in questione come importante, rispetto al totale delle aziende che hanno la possibilità di implementare lo strumento. Lo stesso discorso vale per le percentuali riferite alla modalità di utilizzo, sempre riferita al numero di aziende con la possibilità di implementare lo strumento. Le percentuali d'incrocio tra strumento e fattore causa sono state invece determinate sulla base delle aziende che utilizzano lo strumento (in maniera formale o informale, [SI]) e per cui ha senso la prestazione di sicurezza. Per esempio il 100% che deriva dall'incrocio tra lo strumento 1 e il fattore causa "errata/mancata implementazione delle procedure" per la sicurezza da attacchi, significa che tra tutte le aziende che possono applicare lo strumento (3 aziende non hanno gli strumenti dall' 1 al 4) il 70% lo applica [SI] e, tra quelle che considerano la sicurezza da attacchi, tutte (il 100%) hanno indicato che lo strumento 1 impatta sul fattore causa "errata/mancata implementazione delle procedure". Questo vuol dire che l'impatto del 100% si riferisce a tutte le aziende tranne Ewals, Fercam e VOTG che non hanno gli strumenti dall'1 al 4, BAS, Terminali Italia e Marenzana che non applicano lo strumento [NO] e MDB che non considera la sicurezza da attacchi (il campione è quindi formato dalle restanti 6 aziende che hanno tutte parere concorde). Per stimare l'impatto del fattore causa sul KPI (riga [impatto del fattore causa sul KPI]), avendo ricevuto dalla maggior parte degli intervistati un ordine di importanza relativo tra i fattori causa piuttosto che una percentuale, abbiamo agito nel seguente modo:

[28] Queste considerazioni sono tratte delle opinioni emerse durante le interviste.

- Sicurezza da attacchi. Dai pesi percentuali che alcuni degli intervistati ci hanno fornito per spiegare l'impatto di ogni fattore causa rispetto al numero di furti/manipolazioni subite, ci siamo resi conto che queste erano abbastanza equilibrate, e nessun fattore causa è risultato prevalere nettamente sugli altri. Abbiamo quindi deciso di sfruttare l'ordine di importanza che ci hanno fornito le aziende, assegnando peso 9 al primo fattore causa per impatto sul KPI, peso 4 al secondo e peso 1 al terzo (corrispondente all'ordine fornito elevato alla seconda per accentuare le distanze tra i fattori causa). Sommando i contributi per tutte le aziende e rapportando a cento abbiamo ottenuto le percentuali riportate in Tabella 44.
- Sicurezza di fornitura. Al contrario della sicurezza da attacchi, dai pesi percentuali forniti da alcune aziende ci siamo resi conto che tendenzialmente si spiegano i ritardi al cliente finale con un solo fattore causa (o due al massimo). Per tener conto di questo grosso disequilibrio tra i fattori causa, abbiamo deciso di non considerare l'ordine d'importanza relativo ma di considerare esclusivamente il fattore causa segnalato come il più importante dalle aziende (in alcuni casi ne hanno segnalati due). La percentuale in tabella corrisponde quindi al numero di volte che un'azienda ha segnalato un determinato fattore causa come il più importante, il tutto rapportato a cento. Questo metodo ci ha consentito di mettere in evidenza la forte differenza d'impatto tra il fattore causa considerato più importante e gli altri.

Le percentuali d'incrocio rappresentano la "probabilità di impatto" dello strumento rispetto ad un determinato fattore causa. Percentuali superiori al 50% indicano quindi che più della metà delle aziende che applicano lo strumento hanno individuato il suo impatto su quel determinato fattore causa. Sommando il prodotto tra le probabilità d'impatto di uno strumento sui fattori causa per l'incidenza dei fattori causa sul KPI di sicurezza, si ottiene un'indicazione percentuale dell'influenza dello strumento sul KPI. Sempre in riferimento allo strumento 1 per la sicurezza da attacchi:

$$-0{,}17 \cdot 0{,}26 + 1 \cdot 0{,}38 + 0{,}17 \cdot 0{,}35 = 40\%$$

Questa percentuale esprime la probabilità d'impatto dello strumento 1 sulla sicurezza da attacchi (per l'analisi sugli altri strumenti fare riferimento alla Tabella 46 del paragrafo 6.1).

5.4 Conclusioni

In questo capitolo abbiamo definito la metodologia scelta per lo studio di caso in base ai nostri obiettivi di ricerca. Abbiamo scelto un caso multiplo descrittivo di tipo strumentale per poter esaminare i processi e gli strumenti ricorrenti in aziende simili tra loro; questo ci consentirà, attraverso un ragionamento induttivo, di costruire una teoria generale che possa spiegare l'utilizzo di tali strumenti in funzione dei differenti fattori di contesto. Abbiamo poi scelto l'unità di analisi constatando che due fattori di contesto su sei non potranno essere utili per compiere delle analisi aggiuntive data l'omogeneità del campione. Abbiamo inoltre creato gli strumenti per l'osservazione sul campo in modo tale da garantire chiarezza nell'esposizione delle nostre domande limitando le possibili ambiguità intrinseche negli strumenti culturali proposti. È seguita infine la raccolta dati e la conseguente archiviazione per poter costituire il database di partenza per tutte le analisi che seguiranno nel prossimo capitolo.

6 Analisi ed elaborazione dati

In questo capitolo analizzeremo i dati raccolti tramite le interviste. Questo ci servirà per confermare l'idea alla base del modello proposto nel paragrafo 4.3 e trovare così risposta alle domande di ricerca del paragrafo 4.2. Anzitutto analizzeremo i dati consolidati di tutte le imprese per poter mappare la situazione as-is del settore intermodale in termini di utilizzo, importanza e impatti degli strumenti culturali sui fattori causa e di conseguenza (attraverso l'individuazione della specifica rilevanza di ogni fattore causa) sulle prestazioni di sicurezza.

Svolgeremo successivamente la stessa analisi suddividendo il campione d'imprese in base ai fattori di contesto; questo ci servirà per individuare, in base alle differenze tra le aziende, se esistono delle similitudini o disuguaglianze nell'utilizzo o nella percezione di importanza degli strumenti e dei fattori causa. Queste analisi ci permetteranno, tramite l'integrazione delle informazioni di tipo qualitativo raccolte durante le interviste, di costruire una check-list di strumenti culturali di sicurezza che ogni azienda dovrebbe adottare in relazione ai propri fattori di contesto per poter essere in linea con il mercato.

Abbiamo prodotto delle conclusioni attraverso un confronto analitico dei risultati nei vari casi; questo confronto non si pone l'obiettivo di generalizzare i risultati ad un insieme più ampio (come il campionamento), ma ha come scopo la predizione di risultati simili o dissimili in base a determinate condizioni predefinite (i fattori di contesto). I nostri risultati finali saranno quindi di tipo descrittivo, in accordo con quanto spiegato da Yin (2011): *"lo studio dei casi può essere generalizzabile a delle proposizioni teoriche e non a degli universi […] Lo scopo del ricercatore è di arricchire e di generalizzare delle teorie e non di enumerare delle frequenze"*.

Ai fini dell'analisi, abbiamo tenuto conto di come effettivamente il campione di aziende analizzato tenda ad utilizzare gli strumenti proposti. La classificazione è riportata di seguito nella Tabella 45.

Tabella 45: Modalità di applicazione degli strumenti culturali

Strumento	Modalità di applicazione
(1) Forza lavoro multidisciplinare	Interno
(2) Collaborazione tra dipenenti	Interno
(3) Integrità, lealtà dei dipendenti	Interno
(4) Sviluppo della consapevolezza interna sulla sicurezza	Interno
(5) Aspetti soft	Interno
(6) Continuous improvement	Interno
(7) Business continuity planning	Interno
(8) Segnalare incidenti e debolezze	Interno
(9) Knowledge management	Interno
(10) Valutazione della conformità di sicurezza	Interno/esterno
(11) Partnership	Esterno
(12) Sviluppo della consapevolezza sulla sicurezza con i miei partner	Esterno
(13) Riduzione della differenza di cultura tra azienda e partner	Esterno
(14) Focus sul cliente	Esterno

La Tabella 45 evidenzia la reale modalità di applicazione degli strumenti culturali, e su questa ci baseremo per effettuare le analisi seguenti. Dalle interviste è infatti emerso che generalmente gli strumenti dal 1 al 9 sono applicati esclusivamente con una prospettiva intra-aziendale, con impatti sui processi di una sola azienda; gli strumenti dal 11 al 14 invece, estendono il loro impatto anche fuori dai confini aziendali coinvolgendo i partner di filiera. L'unico strumento che non può essere classificato esclusivamente come interno o esterno è il 10, può essere infatti applicato con una prospettiva esclusivamente interna (quando l'azienda si preoccupa soltanto di essere certificata) oppure esterna (se oltre alla propria certificazioine controlla che lo siano anche i propri partner). Per le successive analisi questo strumento sarà compreso sia negli strumenti interni, che negli strumenti esterni

6.1 Analisi sul totale

6.1.1 Analisi utilizzo-importanza degli strumenti

Di seguito è riportato il grafico che evidenzia il rapporto tra utilizzo e importanza dei 14 strumenti sul quale è focalizzato il nostro lavoro empirico.

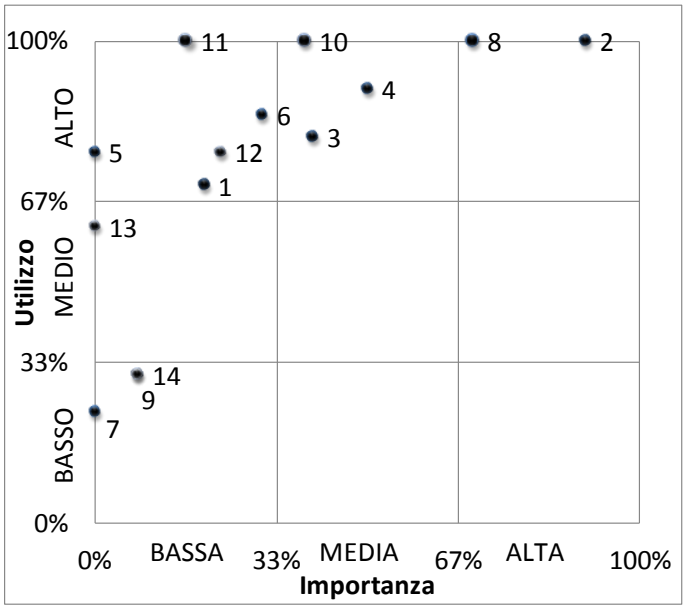


Figura 44: utilizzo/importanza-totale

(1) Forza lavoro multidisciplinare
(2) Collaborazione tra dipendenti
(3) Integrità, lealtà dei dipendenti
(4) Sviluppo della consapevolezza interna sulla sicurezza
(5) Aspetti soft
(6) Continuous improvement
(7) Business continuity planning
(8) Segnalare incidenti e debolezze
(9) Knowledge management
(10) Valutazione della conformità di sicurezza
(11) Partnership
(12) Sviluppo della consapevolezza sulla sicurezza con i miei partner
(13) Riduzione della differenza di cultura tra aziende e partner
(14) Focus sul cliente

Dal grafico si nota come vi sia un gruppo di tre strumenti separati da tutti gli altri, poco utilizzati e considerati poco importanti:

- **Business Continuity Planning:** lo strumento ha una bassa diffusione perché ritenuto difficilmente applicabile nel settore intermodale. Le motivazioni risiedono nelle troppe variabili da dover prevedere per creare dei piani alternativi ex-ante; si preferisce affrontare le disruption progettando alternative in tempo reale. Tra i tanti pareri concordi, Laura Fortina[29] spiega che *"gli imprevisti possibili sono talmente tanti e vari che non è possibile creare procedure alternative formali. I maggiori imprevisti riguardano la puntualità dei treni in arrivo e partenza"*. Il tratto ferroviario è appunto il passaggio più critico per il trasporto intermodale, su cui le aziende hanno meno possibilità di intervento diretto e si devono rimettere all'autorità ferroviaria responsabile della gestione della rete. Come afferma Gianfranco Brillante[30] *"la mancanza di flessibilità delle ferrovie è il punto più critico del trasporto intermodale. […] Quando ci sono grossi imprevisti nella parte ferroviaria, noi siamo completamente in balia dell'operatore ferroviario che a sua volta è in balia del gestore della rete"*. Come vedremo nel paragrafo 6.2.2 le aziende altamente

[29] Laura Fortina, Account manager di Ewals Intermodal
[30] Gianfranco Brillante, Direttore di filiale Fercam

integrate riescono a mitigare questa rigidità potendo intervenire direttamente sulla ripianificazione del tratto su rotaia.

- **Knowledge management:** questo strumento è considerato generalmente poco interessante per il settore e più proficuo per i settori puramente human intensive. Anche le aziende più strutturate non hanno strumenti formali di knowledge management ma fanno ricorso al lavoro di squadra e alla collaborazione per trasmettere la conoscenza. A testimonianza di ciò possiamo riportare le considerazioni di Sergio Crespi[31]:*"non abbiamo uno strumento di questo tipo. Facciamo formazione e istruzione sul campo e il meccanismo del team ci aiuta nella diffusione della conoscenza"*.
- **Focus sul cliente:** questo strumento non è considerato importante nella situazione attuale ma la maggior parte delle aziende ne ha sottolineato la sua potenzialità. Questo perché la filiera è molto spezzettata, e quindi lo strumento risulta di difficile applicazione. Spesso dipende anche dal cliente industriale che è poco interessato a ragionare in ottica di filiera. Sabrina Robba[32] dice che *"la filiera è abbastanza spezzettata […] nei contratti con il cliente l'unico incentivo potrebbe essere quello di incrementare il volume di affari se le prestazioni sono buone"*. Viene però a mancare, da parte del cliente finale o del MTO, un sistema formale di incentivazione tale da garantire in tutti gli anelli della supply chain un'attenzione particolare alla buona riuscita dell'intero processo di filiera.

Da un confronto con la letteratura emergono alcune considerazioni. Per quanto riguarda il BCP, la storia dimostra esempi di successo di questi piani applicati per migliorare la prestazione di sicurezza della supply chain, contribuendo a risollevare in breve tempo le organizzazioni da disruption di notevole rilevanza. Il caso più celebre riguarda il blocco dei traffici aerei che è susseguito all'attacco dell'11 settembre, in cui solo le migliori company americane sono riuscite ad affrontare la situazione critica reindirizzando in breve tempo i traffici via mare e via strada (Williams et al., 2008). Lo stesso Sheffi (2001), tra i programmi suggeriti per rispondere agli attacchi terroristici, parla di piani per la sicurezza specifici per la fornitura in logica di BCP, necessari alle organizzazioni in preparazione a future disruption. Tuttavia in letteratura si evince che il tema è trattato prevalentemente in riferimento alle operation nel loro complesso, piuttosto che nello

[31] Sergio Crespi, Direttore Generale del terminal intermodale di Busto Arsizio/Gallarate

[32] Sabrina Robba, Managing Director di Hoyer Italia e Svizzera e responsabile della sicurezza, ambiente e qualità del gruppo Hoyer

specifico contesto su cui ci siamo focalizzati. Tra i pochi autori che trattano l'applicazione del BCP per la sicurezza del trasporto, Benson (2005) spiega che per la buona applicazione dello strumento, è necessario integrare i BCP con i piani di sicurezza. Osservando l'applicazione dello strumento in termini culturali su un campione di imprese del settore del trasporto, Benson afferma che *"non tutte le organizzazioni hanno programmi di BCP integrati con la sicurezza; alcune di queste possiedono programmi di sicurezza estesi e business continuity planning, ma che interagiscono tra di loro solo quando vengono fatte delle segnalazioni da una delle due parti"*. Tuttavia, Benson ha osservato che le aziende intervistate percepiscono la necessità sia di integrare i programmi di sicurezza al BCP, sia di migliorare i piani stessi: "*alcune aziende hanno forti piani di business continuity, ma li applicano solo a livello di IT; […] altre aziende spendono parecchio tempo e costi sui punti più critici, trascurando quelli meno critici. È necessario reindirizzare focus e sforzi su tutte le possibili aree"*. Nel nostro campione, oltre a mancare completamente l'adozione dello strumento di BCP (11 aziende su 13 non lo applicano), viene a mancare anche una sua percezione positiva (nessuna lo ritiene importante). Alla radice di questa visione potrebbe risiedere una cultura della sicurezza poco sviluppata. In definitiva, la letteratura suggerisce che, dove questo strumento è già applicato in azienda, deve essere esteso a tutte le aree di analisi e in generale essere sviluppato congiuntamente agli altri programmi di sicurezza. In Tabella 73 sono riportate le best practice delle aziende che lo applicano (Hupac e Interporto Rivalta Scrivia) e che dimostrano la fattibilità dell'adozione di questo strumento in un contesto così ricco di variabili, anche solo tramite un'impostazione ad alto livello di piani di BCP (es. assegnando responsabilità specifiche per affrontare una disruption o pensare in anticipo all'utilizzo di modalità di trasporto di backup).

Per quanto riguarda il knowledge management, è ampiamente descritto in letteratura l'importanza di raccogliere e documentare le best practice di una supply chain utili per la gestione dei rischi, e che la realizzazione di un software e delle procedure necessarie per la gestione della conoscenza potrebbe essere ostacolata dai forti investimenti che occorrono per raccogliere e trasformare la conoscenza in forma utile (Rice e Caniato, 2003). Analogamente allo strumento di BCP, lo scarso utilizzo può essere giustificato più da una scarsa percezione dell'importanza di questo strumento (solo 1 su 13 ha detto che è importante) piuttosto che da ragioni economiche o strutturali (nessuna delle piccole aziende lo utilizzano, ma è anche vero che solo la metà delle grandi lo

applicano). L'unica azienda che riconosce l'importanza di questo strumento è Hoyer, che attualmente è l'unica ad utilizzarlo in modo formale, evidenziando una best practice.

Infine, per quanto riguarda il focus sul cliente, lo strumento non è stato considerato importante nella situazione attuale della filiera, e solo alcuni ne hanno identificato le potenzialità. A differenza degli altri due strumenti, la motivazione dello scarso utilizzo risiede effettivamente nei limiti imposti alla filiera intermodale. Si presenta, infatti, molto spezzettata e, sebbene ci possa essere un interesse comune da parte delle aziende a ragionare in ottica di end-to-end supply chain, il limite più grosso è imposto dal cliente industriale, che per primo non premia il raggiungimento di determinati target prestazionali. Tale criticità è emersa anche in letteratura. Gli autori Burmeisters e Solovjovs (2009) confermano quello che è emerso dal nostro campione d'aziende ed identificano i clienti come *"i pionieri di un approccio efficace di SCS integrato lungo la filiera per garantire la sicurezza a livello globale, tale da non ostacolare o rallentare il commercio globale, bensì facilitarlo".* Il cliente finale talvolta è addirittura colui che ostacola l'applicazione di efficaci strumenti per la sicurezza, proprio perché, come detto da Alessandro Negri[33] *"i clienti difficilmente si prendono in carico i costi e la responsabilità di far applicare nuovi strumenti".* Riassumendo è difficile applicare il focus sul cliente per questioni legate alla struttura spezzettata della filiera e per lacune culturali legate al cliente finale; questo strumento potrebbe essere implementato attraverso l'instaurazione di un sistema di valutazione basato su KPI di filiera associati ad incentivi da parte del cliente, come dimostra la best practice di Fercam riportata in Tabella 73.

Dalla Figura 44 si nota inoltre che la maggior parte degli strumenti (1-forza lavoro multidisciplinare, 5-aspetti soft, 6-continuous improvement, 11-partnership, 12-sviluppo della consapevolezza sulla sicurezza con i miei partner) sono molto utilizzati ma percepiti come poco importanti; il motivo è che generalmente sono impiegati per raggiungere obiettivi diversi dalla sicurezza. Meritano un approfondimento gli strumenti esterni 11 e 12 che vengono poco applicati per ragioni culturali (come descritto di seguito nel paragrafo 6.1.2).

Un caso particolare è lo strumento 13-riduzione della differenza di cultura tra azienda e partner che, se utilizzato, rende più efficace lo strumento 11-partnership. Utilizzando lo

[33] Alessandro Negri, Manager Operations di BAS Logistics

strumento 13-riduzione della differenza di cultura tra azienda e partner si ha mediamente un aumento del 30% dell'efficacia dello strumento 11-partnership (6,11 impatti sui fattori causa rispetto a 4,75). A testimonianza di ciò Sergio Crespi[34] dichiara che "*queste iniziative ci servono per migliorare la collaborazione e l'integrazione con i partner e la loro fidelizzazione. Sono iniziative rivolte sia ai nostri clienti che ai nostri fornitori che servono per migliorare la qualità della partnership".*

6.1.2 Analisi importanza dei fattori causa

In Figura 45 si riportano i grafici relativi all'importanza dei fattori causa per la sicurezza da attacchi e quella di fornitura.

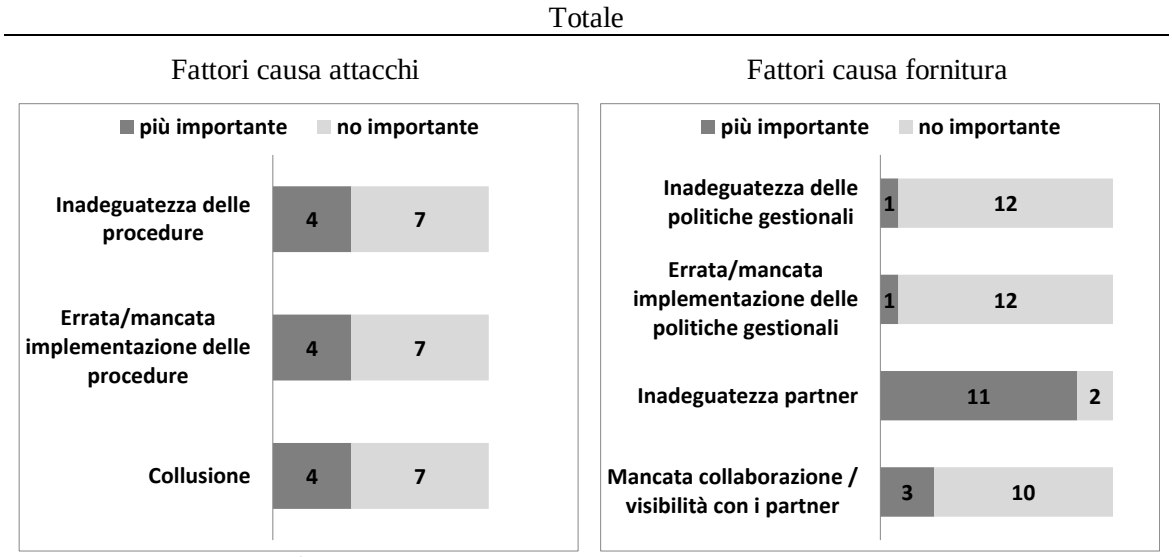


Figura 45: importanza dei fattori causa-totale

Mentre per la sicurezza da attacchi non risulta esserci un fattore causa principale, per la sicurezza di fornitura viene individuata, da quasi tutte le aziende, l'inadeguatezza del partner come prima causa dei ritardi al cliente finale. Come detto da Laura Fortina[35] *"la causa principale dei ritardi […] è imputabile all'inadeguatezza del partner. In particolare è imputabile al tratto su rotaia".*

È interessante notare come, seppur l'inadeguatezza del partner sia considerata la causa principale del ritardo per 11 aziende su 13, gli strumenti esterni siano comunque ritenuti meno importanti di quelli interni (in media le aziende ritengono importanti 3,46[36]

[34] Sergio Crespi, Direttore Generale del terminal intermodale di Busto Arsizio/Gallarate

[35] Laura Fortina, Account manager di Ewals Intermodal

[36] Somma delle percentuali di importanza degli strumenti interni riportati (Tabella 44, colonna [importanza strumento]). Indica il numero di strumenti interni mediamente ritenuti importanti dalle aziende (compreso lo strumento 10); si riferisce quindi ai 10 strumenti interni considerati, può anche essere espresso come percentuale: 35%

strumenti interni contro lo 0,86[37] di quelli esterni). È evidente che, nonostante le aziende si rendano conto di quanto i loro partner siano importanti per raggiungere delle buone prestazioni, facciano ancora fatica a considerare gli strumenti che potrebbero impattare su questo aspetto come determinanti. Il problema è principalmente legato alla tradizione culturale delle aziende che sono abituate a migliorare i problemi interni piuttosto che ragionare sulle prestazioni della filiera.

6.1.3 Analisi impatto degli strumenti sulla sicurezza

La Tabella 46 e la Tabella 47 riportano i 14 strumenti ordinati in base all'impatto che hanno sulla sicurezza da attacchi e di fornitura (per le modalità di calcolo dell'impatto fare riferimento al paragrafo 5.3).

Tabella 46: Totale-sicurezza da attacchi

IMPATTO SULLA SICUREZZA DA ATTACCHI		
11	Partnership	72%
5	Aspetti soft	62%
10	Valutazione della conformità di sicurezza	59%
8	Segnalare incidenti e debolezze	59%
6	Continuous improvement	57%
3	Integrità, lealtà dei dipendenti	50%
2	Collaborazione tra dipendenti	49%
9	Knowledge management	46%
13	Riduzione della differenza di cultura tra aziende e partner	44%
12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	44%
4	Sviluppo della consapevolezza interna sulla sicurezza	43%
1	Forza lavoro multidisciplinare	40%
7	Business continuity planning	12%
14	Focus sul cliente	12%

Tabella 47: Totale-sicurezza fornitura

IMPATTO SULLA SICUREZZA DI FORNITURA		
11	Partnership	72%
12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	55%
10	Valutazione della conformità di sicurezza	53%
9	Knowledge management	52%
13	Riduzione della differenza di cultura tra aziende e partner	47%
8	Segnalare incidenti e debolezze	33%
7	Business continuity planning	29%
6	Continuous improvement	22%
14	Focus sul cliente	20%
2	Collaborazione tra dipendenti	9%
5	Aspetti soft	8%
1	Forza lavoro multidisciplinare	7%
4	Sviluppo della consapevolezza interna sulla sicurezza	7%
3	Integrità, lealtà dei dipendenti	5%

Mentre per la sicurezza da attacchi risulta che la probabilità d'impatto medio di ogni strumento interno è equiparabile a quello di uno esterno (48% degli interni rispetto al 46% degli esterni), per la sicurezza di fornitura gli strumenti esterni hanno una probabilità di impatto medio molto più elevato (49% degli esterni rispetto al 22% degli

[37] Somma delle percentuali di importanza degli strumenti esterni (Tabella 44, colonna [importanza strumento]). Indica il numero di strumenti esterni mediamente ritenuti importanti (compreso lo strumento 10); si riferisce quindi ai 5 strumenti esterni considerati, può anche essere espresso come percentuale: 17%

interni). Si denota quindi un'efficacia maggiore degli strumenti esterni, questo è dovuto al fatto che l'inadeguatezza del partner si è dimostrata il fattore causa principale per la sicurezza di fornitura.

Nello specifico la partnership, considerata dalle aziende poco importante ai fini della sicurezza (Figura 45), risulta invece lo strumento che impatta maggiormente sia sulla sicurezza da attacchi che su quella di fornitura. Questo perché, rispetto ad altri strumenti, ha un raggio d'azione molto più ampio che si estende a tutti i fattori causa proposti (in media la partnership impatta su 5,15 fattori causa su 7, mentre gli altri strumenti hanno un impatto medio su 2,65 fattori causa su 7).

6.2 Analisi in base ai fattori di contesto

Effettueremo di seguito le stesse analisi eseguite sul campione totale di aziende suddividendole però in base alle loro specifiche caratteristiche per quanto riguarda la dimensione, l'integrazione e l'ambito. Utilizzeremo gli ulteriori fattori di contesto individuati paragrafo 4.3.1, per approfondire e discriminare gli strumenti all'interno delle seguenti analisi ove necessario.

6.2.1 Analisi in base al fattore dimensione

Analisi utilizzo-importanza degli strumenti

Di seguito vengono riportati i grafici che evidenziano il rapporto tra utilizzo e importanza dei 14 strumenti analizzati per le aziende grandi e piccole.

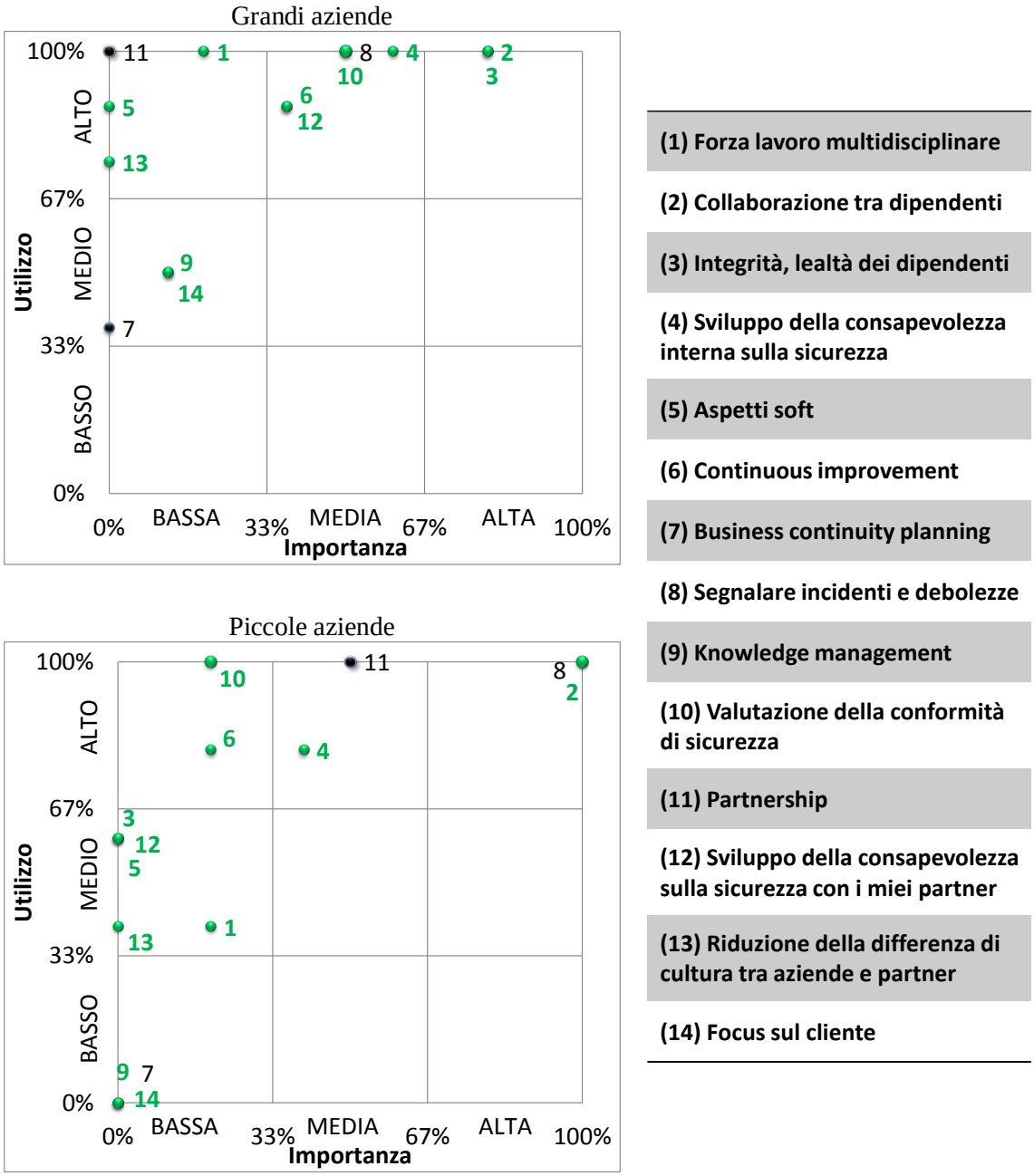


Figura 46: utilizzo/importanza-dimensione

Dalla Figura 46 si nota come in genere le grandi aziende facciano più ampio ricorso agli strumenti culturali di quanto non ne facciano le piccole. Nessuno strumento risulta più utilizzato dalle piccole aziende rispetto alle grandi. Un esempio eclatante è

rappresentato dai tre strumenti discussi nell'analisi del totale (7, 9 e 14) i quali non vengono mai applicati dalle piccole aziende mentre, per quelle di dimensioni maggiori, risultano applicati almeno da 3 aziende su 8 (anche se meno utilizzati rispetto a tutti gli altri strumenti).

Di seguito riportiamo l'analisi dettagliata di tutti gli strumenti per i quali la dimensione risulta essere un fattore discriminante:

(1)	Grandi aziende		Piccole aziende	
Forza lavoro multidisciplinare	Applicazione	100%	Applicazione	40%
	Applicazione formale	100%	Applicazione formale	20%

Tutte le grandi aziende lo applicano in maniera formale (attraverso cioè una modalità standard e definita di utilizzo), mentre per quanto riguarda le piccole aziende solo MDB e TIMO lo applicano, rispettivamente in modo formale e informale (quindi in modo non standardizzato). Seppur questo fattore di contesto discrimina le aziende in modo significativo sull'utilizzo o meno dello strumento (60% di differenza), razionalmente riteniamo che il fattore di contesto "ambito" sia più indicato per spiegare la differenza nell'utilizzo.

(2)	Grandi aziende		Piccole aziende	
Collaborazione tra dipendenti	Applicazione	100%	Applicazione	100%
	Applicazione formale	100%	Applicazione formale	40%

Lo strumento è applicato da tutte le aziende. La differenza tra piccole e grandi risiede nella modalità di applicazione: la totalità delle grandi aziende lo utilizza in maniera formale, mentre solo 2 aziende piccole su 5 lo utilizzano formalmente. Ad esempio Sergio Crespi[38] spiega che l'azienda possiede *"un'ingegneria turnistica articolatissima per cui il team viene creato tenendo conto delle caratteristiche delle persone […] il sistema* (informatico) *fa questo calcolo particolare".* Un'altra azienda grande come Interporto di Rivalta Scrivia ha un amministratore delegato che si occupa esclusivamente della formazione e gestione delle risorse umane *"il riferimento alla squadra è sempre presente. C'è un controllo costante perché gestire 650 addetti non è*

[38] Sergio Crespi, Direttore Generale del terminal intermodale di Busto Arsizio/Gallarate

un compito facile e nel confronto quotidiano con le direzioni operative viene deciso se spostare o meno una persona in un'altra unità operativa, se questa non rende come desiderato o potrebbe rendere di più in un altro contesto"[39]. Per le piccole aziende risulta più semplice gestire il lavoro di squadra in modo informale dato il numero più ristretto di persone, come espresso da Aldo Locurcio[40] *"All'inizio la collaborazione e il lavoro in team sono necessari per i nuovi arrivati, ma poi col tempo ognuno si specializza nella sua mansione e sulle proprie responsabilità e il team diventa più una conseguenza del lavoro piuttosto che un elemento progettato".*

(3)	**Grandi aziende**		**Piccole aziende**	
Integrità, lealtà dei dipendenti	Applicazione	100%	Applicazione	60%
	Applicazione formale	80%	Applicazione formale	40%

Lo strumento è applicato da tutte le grandi aziende (4 su 5 in modo formale), mentre per le piccole aziende la percentuale d'utilizzo scende al 60% (2 su 5 formalmente). È interessante notare come, oltre all'applicazione, anche la percezione delle aziende sull'importanza dello strumento cambi radicalmente tra i due cluster: l'80% (4 su 5) delle grandi aziende ritiene lo strumento tra i più importanti, mentre nessuna piccola azienda lo ritiene tale. Il motivo è da ricercare nella differente struttura organizzativa che porta le piccole aziende ad avere un controllo diretto dei propri operatori da parte del management, mentre per aziende grandi questo controllo diventa a mano a mano più debole e quindi risulta molto importante uno strumento ad hoc per incrementare la lealtà e l'integrità dei dipendenti. Infatti, come testimoniano le parole di Fabrizio Filippi[41], in riferimento all'implementazione di un sistema di integrità e fidelizzazione dei dipendenti unito alla collaborazione, *"Una volta che c'è questo il 90% è fatto perché vuol dire che si è riusciti trasmettere la filosofia dell'intera azienda".*

(4)	**Grandi aziende**		**Piccole aziende**	
Sviluppo della consapevolezza interna sulla sicurezza	Applicazione	100%	Applicazione	80%
	Applicazione formale	100%	Applicazione formale	60%

[39] Frase estrapolate dall'intervista a Gianluca Fossati, Ufficio Sales e Marketing di Interporto Rivalta Scrivia

[40] Aldo Locurcio, Responsabile del terminal intermodale di Segrate di Terminali Italia

[41] Fabrizio Filippi, Direttore operativo di Sogemar

Le uniche aziende che non applicano questo strumento in modo formale sono Terminali Italia e TI.MO (l'unica azienda a non utilizzarlo). Sono entrambe piccole aziende e il motivo risiede nel fatto che, essendo meno strutturate e con un numero ristretto di dipendenti, non hanno la necessità di instituire riunioni per diffondere tematiche di sicurezza. Come afferma Davide Muzio[42] *"essendo piccoli è facile, perché si tratta di istruire poche persone, che oltretutto sono sempre controllate da un supervisore. La sicurezza è un aspetto più delicato nelle organizzazioni più complesse, dove le procedure sono viste talvolta come un rallentamento".*

Il fattore di contesto dimensione non spiega però in modo esaustivo l'applicazione dello strumento 4; rimandiamo all'analisi del fattore ambito per approfondimenti.

(5)	**Grandi aziende**		**Piccole aziende**	
Aspetti soft	Applicazione	88%	Applicazione	60%
	Applicazione formale	75%	Applicazione formale	40%

Vengono utilizzati maggiormente nelle aziende grandi (delta del 28%) in quanto implementare un programma completo di corporate governance è una scelta effettuata prevalentemente da imprese strutturate. Bruno Carbonin[43], lavorando in una piccola azienda, afferma che *"attualmente non abbiamo strumenti di questo tipo. […] In ogni caso penso che questo tipo di codici nelle grandi aziende possano avere un impatto sulla motivazione dei dipendenti, ma per un'azienda come la nostra la comunicazione e il rapporto personale è sicuramente più importante"*. Nelle grandi aziende, dato che il rapporto personale tra dirigenza e lato operativo è meno stretto, la tendenza è quella di utilizzare lo strumento in modo formale; come spiegato da Sergio Crespi[44] *"si cerca di stare attenti a quegli aspetti che riguardano il simbolismo, il mito e questo tipo di cose, spesso ripresi nelle nostre riunioni. Cerchiamo di portare avanti determinati linguaggi, motti, o esempi di comportamenti che divulghiamo anche con l'aiuto di slide o filmati che mirano a creare dell'identificazione nei confronti dell'azienda da parte del lavoratore".*

[42] Davide Muzio, Consigliere Delegato di TIMO
[43] Bruno Carbonin, Direttore di MDB
[44] Sergio Crespi, Direttore Generale del terminal intermodale di Busto Arsizio/Gallarate

Inoltre per le aziende quotate dotarsi di un codice etico all'interno del programma di corporate governance è oggigiorno una prassi, per fornire garanzia di trasparenza e visibilità agli investitori, e per seguire le direttive del codice di autodisciplina.

(6)	**Grandi aziende**		**Piccole aziende**	
Continuous improvement	Applicazione	88%	Applicazione	80%
	Applicazione formale	50%	Applicazione formale	0%

Non esiste un grosso gap a livello di utilizzo, ma vi è una netta differenza nella modalità di applicazione. La dimensione piccola consente di gestire il processo di miglioramento continuo più agevolmente (tutte le aziende che lo utilizzano lo fanno in maniera informale) dato lo stretto contatto tra lato manageriale e operativo.
Nelle grandi aziende invece la tendenza è quella di utilizzarlo in maniera formale (3 su 5).

(7)	**Alta integrazione**		**Bassa integrazione**	
Business continuity planning	Applicazione	38%	Applicazione	0%
	Applicazione formale	38%	Applicazione formale	0%

Nessuna azienda di piccole dimensioni applica lo strumento, questo perché manca loro la forza contrattuale per influenzare il trazionista. È infatti proprio questa possibilità che consente di stilare un action plan a seguito di disruption. Per le piccole aziende il problema legato al tratto ferroviario è fortemente avvertito, come spiegato da Alessandro Negri[45]: *"essendo il punto di riferimento per il cliente, spesso abbiamo a che fare con reclami per problematiche non causate direttamente da noi. Per esempio quando un treno si ferma, non abbiamo alcun margine per intervenire, ma il cliente si rifà su di noi. Ad oggi, per un'azienda come la nostra, è questo il vero limite del trasporto intermodale".*

[45] Alessandro Negri, Manager Operations di Bas Logistic

(9)	Grandi aziende		Piccole aziende	
Knowledge management	Applicazione	50%	Applicazione	0%
	Applicazione formale	13%	Applicazione formale	0%

Lo strumento è utilizzato da Hoyer, Interporto Rivalta Scrivia, VOTG e Fercam (solo Hoyer in modo formale), tutte grandi aziende. Il motivo del non utilizzo da parte delle piccole aziende risiede in due fattori. Il primo è che lo strumento non è tipico del settore, perché utilizzato principalmente dove il capitale umano è il fattore critico di successo (le piccole aziende si concentrano quindi su strumenti relativi al proprio core business). Il secondo motivo riguarda invece la varietà di casistiche e il numero di persone necessarie per poter giustificare da un lato l'investimento in un software di knowledge management, e dell'altro il tempo dedicato alla codifica delle esperienze.

(10)	Grandi aziende		Piccole aziende	
Valutazione della conformità di sicurezza	Applicazione	100%	Applicazione	100%
	Applicazione formale	100%	Applicazione formale	40%

Questo strumento è applicato dalla totalità del campione di aziende analizzato, ma vi è una correlazione riguardo alla modalità di applicazione in base alla dimensione dell'azienda. Tutte le aziende di grandi dimensioni, oltre ad avere e richiedere certificazioni specifiche, adottano un meccanismo formale per la valutazione della sicurezza dei processi interni e dei propri partner. Ad esempio Fabrizio Filippi[46] afferma: *"Abbiamo degli ispettori interni che fanno dalle due alle tre visite all'anno ai nostri fornitori; da lì vengono redatte le non conformità per quanto riguarda tutti i processi, da come fa la fattura a come riceve la merce. Se il partner dichiara di avere il piazzale satellitato e poi non ce l'ha per noi questa è una grave non conformità".* Per quanto riguarda le piccole, solo 2 su 5 sfruttano un sistema di valutazione formale, ma, anche laddove viene utilizzato questo tipo di sistema, non abbiamo mai riscontrato delle ispezioni verso i partner.

Così come per il continous improvement, la dimensione dell'azienda è correlata alla modalità di applicazione dello strumento.

[46] Fabrizio Filippi, Direttore operativo di Sogemar

(12)	Grandi aziende		Piccole aziende	
Sviluppo della consapevolezza sulla sicurezza con i miei partner	Applicazione	88%	Applicazione	60%
	Applicazione formale	63%	Applicazione formale	40%

Questo strumento viene maggiormente applicato dalle grandi aziende (7 aziende lo applicano di cui 3 formalmente su 8), mentre per quanto riguarda le piccole aziende solo Marenzana, MDB e TI.MO. lo applicano (quest'ultima in modo informale) su 5. Anche se la differenza percentuale non è molto pronunciata riteniamo che la dimensione spieghi in parte l'utilizzo di questo strumento (questo strumento sarà poi spiegato nel paragrafo 6.2.3). Infatti è più probabile per le grandi aziende essere la focal company della filiera e quindi avere la necessità di sviluppare in modo formale le competenze e la consapevolezza sulle tematiche di sicurezza dei loro partner, spesso più piccoli e meno strutturati.

Ad esempio *Hupac si pone come promotore delle iniziative di formazione continua in relazione alla sicurezza all'interno della filiera, e molto spesso si assume anche il compito di educare i partner per ottenere prestazioni di filiera migliori.*[47] Questo strumento viene applicato dalle grandi aziende anche verso partner di dimensioni comparabili come ci conferma Laura Fortina[48]: *"Ewals organizza dei meeting con le maggiori ditte che offrono servizi di trasporto stradale con lo specifico tema della sicurezza. In questi meeting i nostri responsabili si ritrovano insieme ai responsabili delle ditte di trazione e agli autisti e cercano di far capire al meglio la nostra metodologia di lavoro. Sicuramente queste occasioni sono utili per far crescere la consapevolezza su alcune tematiche di sicurezza per noi fondamentali per poter offrire un servizio di qualità".*

Mentre per quanto riguarda piccole aziende, come BAS o Terminali Italia, vengono effettuati sforzi nella formazione e sviluppo della consapevolezza solo verso i dipendenti interni all'azienda.

[47] Frase tratta dalla scheda dell'intervista effettuata a Sergio Crespi, Direttore Generale del terminal HUPAC di Busto Arsizio/Gallarate

[48] Laura Fortina, Account manager di Ewals Intermodal

(13)	Grandi aziende		Piccole aziende	
Riduzione della differenza di cultura tra azienda e partner	Applicazione	75%	Applicazione	40%
	Applicazione formale	63%	Applicazione formale	20%

L'applicazione dello strumento 13 è maggiore per le grandi aziende (6 su 8, di cui 5 formalmente) rispetto a quelle di piccole dimensioni (2 su 5, di cui solo 1 formalmente). Come per lo strumento 12, le piccole aziende lo implementano in misura minore e, laddove lo implementano, quasi sempre in modo informale perché sono rivolte di più ai loro processi interni, al contrario delle grandi aziende nelle quali vi è un'attenzione maggiore per quelle che sono le problematiche di filiera e di integrazione. Queste aziende sono le sole ad avere la capacità e i mezzi per poter migliorare le prestazioni e spesso sono anche i responsabili della prestazione finale di sicurezza agli occhi del cliente. Come approfondiremo nella sezione dedicata all'analisi sul fattore ambito è proprio l'interfaccia con il cliente la variabile che spinge le aziende all'utilizzo di questo strumento; la dimensione invece influisce più che altro sulla modalità di applicazione.

(14)	Grandi aziende		Piccole aziende	
Focus sul cliente	Applicazione	50%	Applicazione	0%
	Applicazione formale	0%	Applicazione formale	0%

Questo strumento, in generale poco applicato, non viene mai applicato da piccole aziende. Il motivo risiede nel fatto che solo aziende di una certa dimensione hanno la possibilità di esercitare un'influenza sulle altre; l'obiettivo è quello di creare un processo di filiera integrato che abbia come ultimo obiettivo la soddisfazione del cliente finale. In riferimento a Marenzana (piccola azienda), Francesca Doria[49] afferma che *"vediamo il treno come un mezzo, ne conosciamo gli orari di partenza e arrivo, il numero di treni al giorno, le tracce ecc., però non lo riteniamo parte integrante del nostro processo. Ci limitiamo a fare riservazioni ed eventualmente dei reclami per mancato servizio"*. Questo testimonia il fatto che Marenzana non ha la possibilità di influenzare il trazionista ferroviario per farlo lavorare con l'ottica del cliente finale. Mentre per una grande azienda come Ewals, l'approccio è differente come ci spiega

[49] Francesca Doria, Operational Manager di Marenzana

Laura Fortina[50] *"negli incontri è importante per noi far arrivare ai nostri partner il messaggio che tutti siamo parte di una filiera fatta da tanti attori con responsabilità differenti, e che il lavoro di ogni attore è indispensabile e condiziona anche tutti gli altri"*.

In generale le aziende di grandi dimensioni presentano una percentuale di applicazione degli strumenti culturali maggiore (in media vengono utilizzati 11,75 strumenti su 14 di cui 9,3 in modo formale) rispetto alle piccole aziende (le quali applicano in media 8,2 strumenti di cui 4,4 in maniera formale). Questo perché, ricordando che la dimensione è stata calcolata in base al numero di dipendenti e il fatturato, la maggiore strutturazione aziendale determina la necessità del loro utilizzo, e la maggiori disponibilità economica favorisce l'adozione formale di tali strumenti (software specifici, programmi e iniziative a frequenza continua).

Il fattore di contesto "dimensione" è stato utile per spiegare l'utilizzo dei seguenti strumenti: 2-collaborazione tra dipendenti, 3-integrità/lealtà dei dipendenti, 4-sviluppo della consapevolezza interna sulla sicurezza, 5-aspetti soft, 6-continuous improvement, 9-knowledge management, 10-valutazione della conformità di sicurezza, 12-sviluppo della consapevolezza con i miei partner, 13-riduzione della differenza di cultura tra azienda e partner, 14-focus sul cliente.

Analisi importanza dei fattori causa

In Figura 47 si riportano i grafici relativi all'importanza dei fattori causa per la sicurezza da attacchi e quella di fornitura per le grandi e piccole aziende.

[50] Laura Fortina, Account manager di Ewals Intermodal

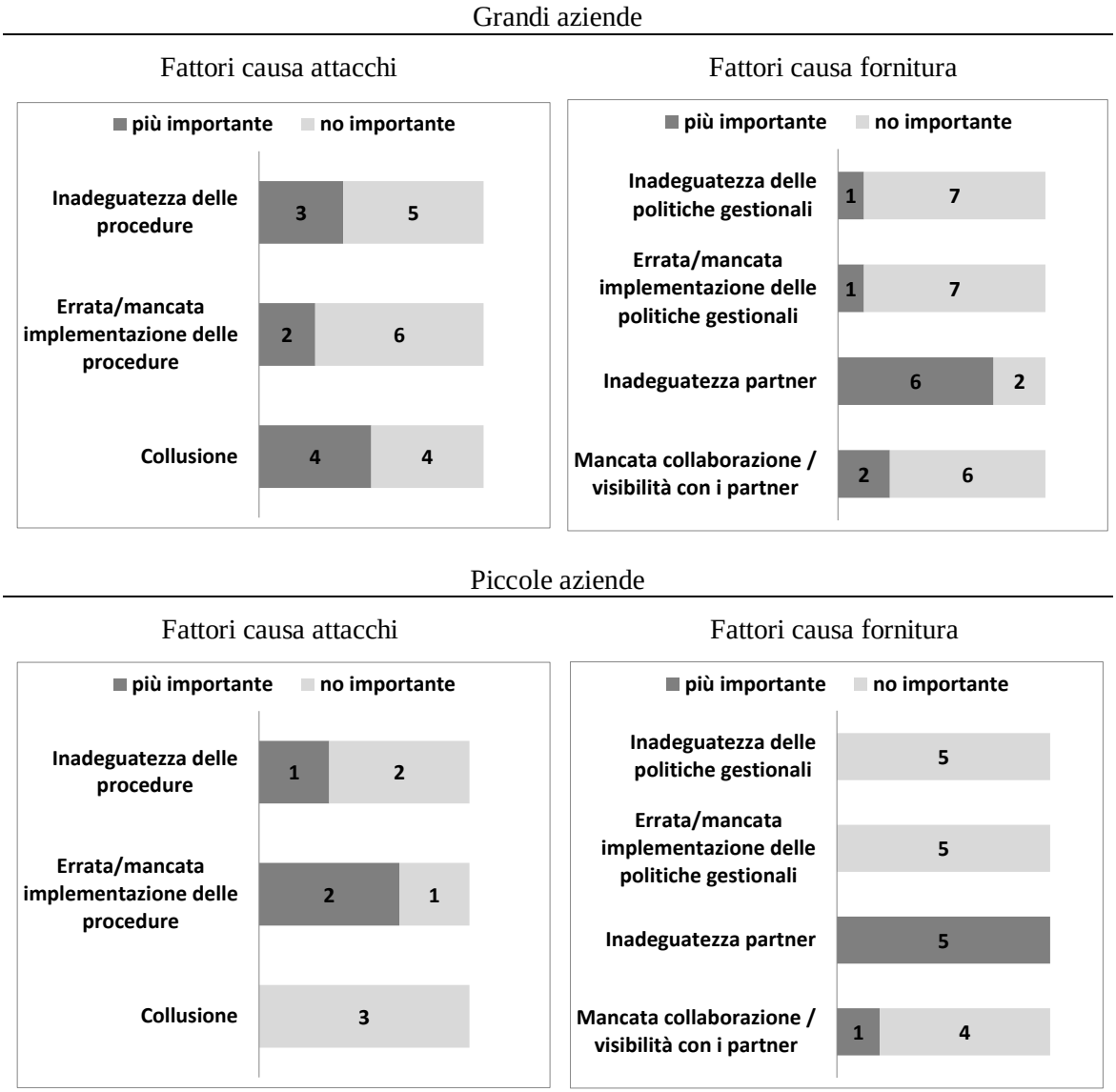


Figura 47: importanza dei fattori causa-dimensione

Si può osservare come dal punto di vista della sicurezza da attacchi le piccole aziende non individuino nella collusione una possibile problematica; questo probabilmente può essere spiegato dal rapporto più stretto tra dirigenza e singolo dipendente. Nelle grandi aziende invece, la collusione rappresenta la prima causa rispetto a furti e manipolazioni della merce. Il motivo risiede nel fatto che esistono procedure di sicurezza più accurate e sistemi di controllo più efficaci, per cui l'episodio collusivo risulta essere il punto debole, dato anche il rapporto più distante tra dirigenza e operatori. A testimonianza di ciò, la percentuale di aziende che ritengono importante lo strumento integrità, lealtà dei dipendenti varia molto come evidenziato precedentemente nella spiegazione di tale strumento.

Per quanto riguarda la sicurezza di fornitura, l'inadeguatezza del partner è ritenuta da entrambe le categorie la causa principale anche se c'è una differenza sostanziale nei numeri. Infatti se tutte le piccole aziende ritengono questa la causa principale (5 su 5), per le grandi aziende questa proporzione scende (6 su 8); probabilmente il motivo di questa difformità deriva dal fatto che le grandi aziende, dato il maggior potere contrattuale, possono influenzare il modus operandi del partner, anche se si tratta del trazionista ferroviario.

Analisi impatto degli strumenti sulla sicurezza

La Tabella 48 e la Tabella 49 riportano i 14 strumenti ordinati in base all'impatto che hanno sulla sicurezza da attacchi rispettivamente per le aziende grandi e piccole.

Tabella 48: Grandi aziende

IMPATTO SULLA SICUREZZA DA ATTACCHI PER AZIENDE DI GRANDI DIMENSIONE		
11	Partnership	77%
10	Valutazione della conformità di sicurezza	65%
5	Aspetti soft	65%
8	Segnalare incidenti e debolezze	50%
3	Integrità, lealtà dei dipendenti	49%
12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	48%
2	Collaborazione tra dipendenti	47%
13	Riduzione della differenza di cultura tra aziende e partner	45%
6	Continuous improvement	45%
4	Sviluppo della consapevolezza interna sulla sicurezza	42%
9	Knowledge management	40%
1	Forza lavoro multidisciplinare	36%
7	Business continuity planning	10%
14	Focus sul cliente	8%

Tabella 49: Piccole aziende

IMPATTO SULLA SICUREZZA DA ATTACCHI PER AZIENDE DI PICCOLA DIMENSIONE		
6	Continuous improvement	95%
8	Segnalare incidenti e debolezze	95%
11	Partnership	54%
3	Integrità, lealtà dei dipendenti	46%
5	Aspetti soft	46%
2	Collaborazione tra dipendenti	44%
1	Forza lavoro multidisciplinare	41%
4	Sviluppo della consapevolezza interna sulla sicurezza	41%
10	Valutazione della conformità di sicurezza	27%
13	Riduzione della differenza di cultura tra aziende e partner	0%
7	Business continuity planning	0%
9	Knowledge management	0%
12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	0%
14	Focus sul cliente	0%

Dal confronto delle probabilità di impatto degli strumenti sulla sicurezza da attacchi ne emerge una differenza sostanziale: per le grandi aziende in media gli strumenti esterni hanno una probabilità di miglioramento del 49% (rispetto al 45% di quelli interni), mentre nel caso di piccole aziende la probabilità crolla al 16% (molto più bassa rispetto al potenziale impatto di quelli interni del 44%). Questo può essere spiegato dal fatto che una cattiva prestazione lato attacchi per una grande azienda è migliorabile applicando strumenti esterni come partnership, valutazione delle conformità di sicurezza, sviluppo della consapevolezza sulla sicurezza con i partner, etc. L'azione di miglioramento è

quindi rivolta verso gli altri attori della filiera i quali saranno probabilmente più piccoli e più vulnerabili. Per le piccole aziende invece il miglioramento è dato principalmente dall'applicazione di strumenti interni quali continuous improvement e segnalare incidenti e debolezze con ottica esclusivamente internai. Si evince quindi come per una grande azienda (ai fini della sicurezza da attacchi) siano molto più importanti gli strumenti esterni, mentre per una piccola siano più importanti quelli interni.
La Tabella 50 e la Tabella 51 riportano i 14 strumenti ordinati in base all'impatto che hanno sulla sicurezza di fornitura per aziende grandi e piccole.

Tabella 50: Grandi aziende

IMPATTO SULLA SICUREZZA DI FORNITURA PER AZIENDE DI GRANDI DIMENSIONE		
11	Partnership	80%
13	Riduzione della differenza di cultura tra aziende e partner	56%
9	Knowledge management	52%
10	Valutazione della conformità di sicurezza	52%
12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	47%
6	Continuous improvement	31%
7	Business continuity planning	30%
8	Segnalare incidenti e debolezze	30%
14	Focus sul cliente	23%
2	Collaborazione tra dipendenti	14%
1	Forza lavoro multidisciplinare	11%
4	Sviluppo della consapevolezza interna sulla sicurezza	11%
5	Aspetti soft	10%
3	Integrità, lealtà dei dipendenti	5%

Tabella 51: Piccole aziende

IMPATTO SULLA SICUREZZA DI FORNITURA PER AZIENDE DI PICCOLA DIMENSIONE		
12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	80%
10	Valutazione della conformità di sicurezza	60%
11	Partnership	47%
8	Segnalare incidenti e debolezze	40%
13	Riduzione della differenza di cultura tra aziende e partner	10%
14	Focus sul cliente	0%
1	Forza lavoro multidisciplinare	0%
2	Collaborazione tra dipendenti	0%
3	Integrità, lealtà dei dipendenti	0%
4	Sviluppo della consapevolezza interna sulla sicurezza	0%
5	Aspetti soft	0%
6	Continuous improvement	0%
7	Business continuity planning	0%
9	Knowledge management	0%

Per la sicurezza di fornitura risultano più importanti gli strumenti esterni sia per le grandi aziende (probabilità d'impatto degli strumenti esterni pari a 51% contro il 25% degli interni), sia per le piccole aziende (probabilità d'impatto degli strumenti esterni pari a 39% contro il 10% degli interni). Si può constatare che, per le piccole aziende, 9 strumenti (di cui 8 interni) sui 14 totali non hanno impatti sul ritardo al cliente finale.

6.2.2 Analisi in base al fattore integrazione

Analisi utilizzo-importanza degli strumenti

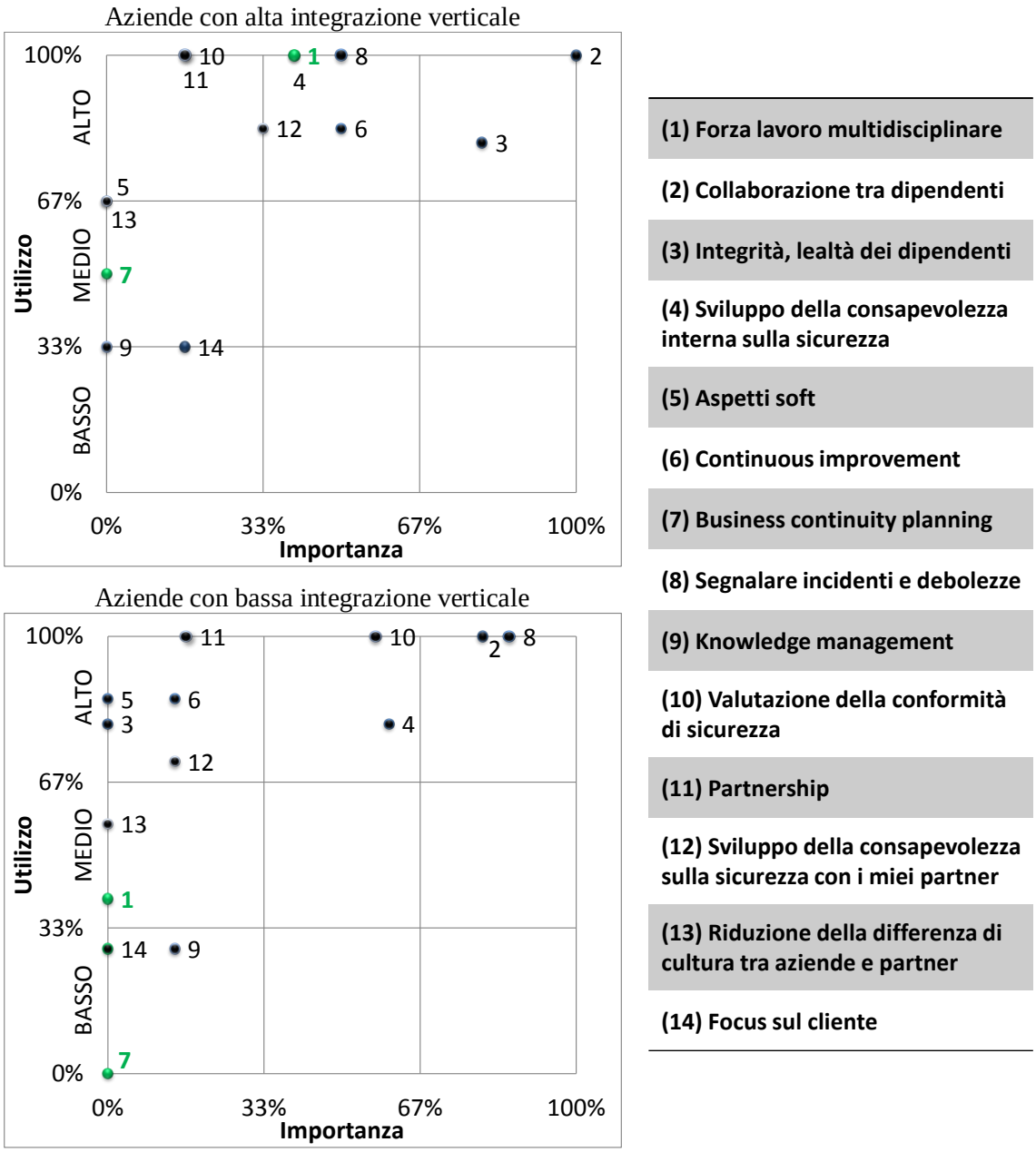


Figura 48: utilizzo/importanza-integrazione

Di seguito riportiamo l'analisi dettagliata di tutti gli strumenti per i quali l'integrazione risulta essere un fattore discriminante:

(1)	Alta integrazione		Bassa integrazione	
Forza lavoro multidisciplinare	Applicazione	100%	Applicazione	40%
	Applicazione formale	100%	Applicazione formale	20%

Come si nota dalla Figura 48, aumentando l'integrazione verticale, lo strumento 1, oltre ad essere più utilizzato, viene anche percepito come più importante. Questo perché le aziende con un'alta integrazione verticale, inglobando più attività nella filiera intermodale, necessitano di operatori in grado di conoscere e capire più problematiche legate alle diverse fasi del processo di trasporto. Per un'azienda molto integrata, come spiegato da Gianluca Fossati[51], "*c'è sicuramente questo discorso di formare gli operatori non solo sul loro lavoro specifico. Questo anche perché la nostra è un'azienda molto complessa che deve fare diverse attività, e avere una visione d'insieme aiuta quando c'è un problema da affrontare"*. Invece un manager[52] di un'azienda poco integrata come Marenzana afferma che "a*gli autisti interessa fino a un certo punto da che cliente poi dovrà andare il container. Loro sanno per quale destinazione devono portare il container, così che possano fare un controllo della prenotazione fatta in precedenza, e questo è importante che lo facciano. Per il resto dar loro una formazione a più ampio spettro non penso sia importante".*

(7)	Alta integrazione		Bassa integrazione	
Business continuity planning	Applicazione	50%	Applicazione	0%
	Applicazione formale	50%	Applicazione formale	0%

Questo strumento è direttamente collegato alla possibilità dell'azienda di influenzare le scelte del trazionista. Infatti, le sole aziende che hanno questo strumento sono Hupac, Interporta Rivalta Scrivia e VOTG le quali (loro stesse o le loro capogruppo) gestiscono anche la trazione ferroviaria. Invece MDB e Terminali Italia, le cui capogruppo si occupano di trazione, sono troppo piccole per poterle influenzare. In ogni caso poter influire in qualche modo sulle scelte di trazione consente di stabilire a priori delle tratte ferroviarie alternative in caso di disruption sulla linea classica (con degli action plan). Sergio Crespi[53], facente parte di un'azienda altamente integrata lato ferrovia, ci ha

[51] Gianluca Fossati, Ufficio Sales e Marketing di Interporto Rivalta Scrivia
[52] Francesca Doria, operational manager di Marenzana
[53] Sergio Crespi, Direttore Generale del terminal intermodale di Busto Arsizio/Gallarate

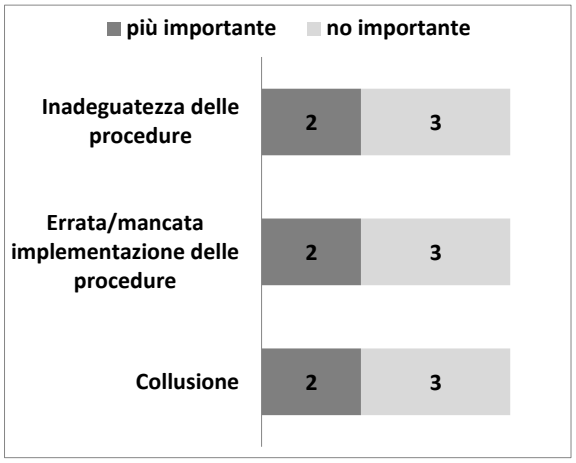
fornito un esempio in questo senso: *"Noi abbiamo delle unità di crisi soprattutto a livello di manager degli assi ferroviari a Chiasso che valutano tutte queste situazioni* (disruption). *Un esempio eclatante recente è stata la chiusura di una direttrice del tunnel del Sempione per un incendio; abbiamo dovuto sfruttare una linea di trasporto diversa che passa da Chiasso piuttosto che da Luino, che è la nostra linea classica. È quindi evidente che noi ci teniamo sempre delle soluzioni alternative per ovviare a queste situazioni".* Invece, come già testimoniato nel paragrafo 6.1 da Gianfranco Brillante[54], le aziende poco integrate (non avendo un controllo diretto sul vettore ferroviario, né tanto meno sul gestore della rete o sull'operatore commerciale logistico) rimangono in balia delle scelte di chi si occupa della tratta ferroviaria.
Il fattore di contesto "integrazione" è stato utile per spiegare l'utilizzo degli strumenti 1, 7, 14.

Analisi importanza dei fattori causa

In Figura 49 si riportano i grafici relativi all'importanza dei fattori causa per la sicurezza da attacchi e quella di fornitura per le aziende con alta e bassa integrazione.

Aziende con alta integrazione verticale

Fattori causa attacchi



Fattori causa fornitura

[54] Gianfranco Brillante, Direttore di filiale Fercam

Aziende con bassa integrazione verticale

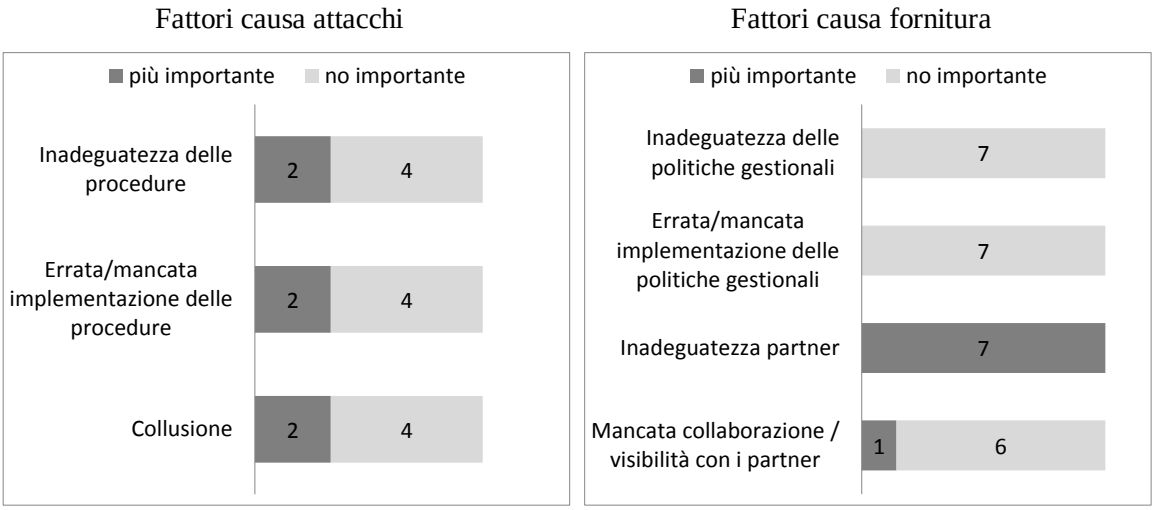


Figura 49: importanza dei fattori causa-integrazione

Si evidenzia come le cause della prestazione sicurezza da attacchi siano percepite in modo bilanciato (non vi è nessuna causa che da sola spieghi gran parte della prestazione), sia per le aziende fortemente integrate sia per quelle con bassa integrazione. Per quanto riguarda la prestazione di sicurezza di fornitura l'ordine relativo di importanza dei fattori causa è il medesimo tra aziende molto o poco integrate. Da un'analisi quantitativa si evince però che tutte le aziende con bassa integrazione hanno individuato nell'inadeguatezza del partner la causa principale, mentre per le aziende più integrate "solo" 4 su 6 hanno menzionato questo fattore causa tra i più importanti. La spiegazione risiede proprio nel fatto che le aziende fortemente integrate possono influenzare la tratta ferroviaria perché di loro responsabilità o della capogruppo; questo da un lato consente di migliorare cattive prestazioni legate al tratto ferroviario, dall'altro (laddove non vi siano miglioramenti) le responsabilità non sono più imputabili ai partner ma ricadono internamente.

Analisi impatto degli strumenti sulla sicurezza

La Tabella 52 e la Tabella 53 riportano i 14 strumenti ordinati in base all'impatto che hanno sulla sicurezza da attacchi rispettivamente per le aziende con alta e bassa integrazione.

Tabella 52: Aziende con alta integrazione

IMPATTO SULLA SICUREZZA DA ATTACCHI PER AZIENDE MOLTO INTEGRATE		
11	Partnership	93%
5	Aspetti soft	79%
8	Segnalare incidenti e debolezze	75%
10	Valutazione della conformità di sicurezza	65%
6	Continuous improvement	60%
2	Collaborazione tra dipendenti	51%
12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	48%
1	Forza lavoro multidisciplinare	46%
4	Sviluppo della consapevolezza interna sulla sicurezza	46%
13	Riduzione della differenza di cultura tra aziende e partner	43%
9	Knowledge management	39%
3	Integrità, lealtà dei dipendenti	35%
7	Business continuity planning	14%
14	Focus sul cliente	-11%

Tabella 53: Aziende con bassa integrazione

IMPATTO SULLA SICUREZZA DA ATTACCHI PER AZIENDE POCO INTEGRATE		
3	Integrità, lealtà dei dipendenti	70%
10	Valutazione della conformità di sicurezza	57%
6	Continuous improvement	54%
11	Partnership	52%
13	Riduzione della differenza di cultura tra aziende e partner	50%
5	Aspetti soft	50%
9	Knowledge management	50%
2	Collaborazione tra dipendenti	48%
8	Segnalare incidenti e debolezze	45%
4	Sviluppo della consapevolezza interna sulla sicurezza	40%
12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	35%
14	Focus sul cliente	35%
1	Forza lavoro multidisciplinare	26%
7	Business continuity planning	0%

Dal confronto delle probabilità medie di impatto degli strumenti emerge che sia quelli esterni che quelli interni concorrono in modo pressoché uguale al miglioramento della prestazione di sicurezza da attacchi. Non vi è inoltre alcuna differenza tra imprese integrate o non integrate: per le aziende integrate in media gli strumenti esterni hanno una probabilità di miglioramento del 48% (rispetto il 51% di quelli interni), mentre nel caso di aziende poco integrate la probabilità va al 46% (rispetto il 44% di quelli interni). Una possibile anomalia è rappresentata dal fatto che per le aziende integrate la partnership abbia un impatto notevole. In realtà nel nostro campione non esistono società totalmente integrate; ad esempio Sogemar (società che ricopre il ruolo di MV e GO) si affida per la parte stradale oltre che a vettori interni anche a padroncini esterni. Si spiega quindi il perché per l'azienda, per garantire prestazioni comparabili a quelle raggiunte dai vettori interni, lo strumento partnership abbia un notevole impatto. Si nota come per le aziende poco integrate ci sia un impatto molto elevato della lealtà/integrità dei dipendenti mentre per quelle con alta integrazione lo strumento 14 abbia un impatto negativo sulla sicurezza da attacchi.

La

Tabella 54 e la Tabella 55 riportano i 14 strumenti ordinati in base all'impatto che hanno sulla sicurezza di fornitura rispettivamente per le aziende con alta e bassa integrazione.

Tabella 54: Aziende con alta integrazione

IMPATTO SULLA SICUREZZA DI FORNITURA PER AZIENDE MOLTO INTEGRATE		
11	Partnership	88%
13	Riduzione della differenza di cultura tra aziende e partner	63%
10	Valutazione della conformità di sicurezza	56%
9	Knowledge management	50%
8	Segnalare incidenti e debolezze	40%
14	Focus sul cliente	38%
12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	33%
6	Continuous improvement	30%
7	Business continuity planning	29%
2	Collaborazione tra dipendenti	20%
5	Aspetti soft	16%
1	Forza lavoro multidisciplinare	15%
4	Sviluppo della consapevolezza interna sulla sicurezza	15%
3	Integrità, lealtà dei dipendenti	6%

Tabella 55: Aziende con bassa integrazione

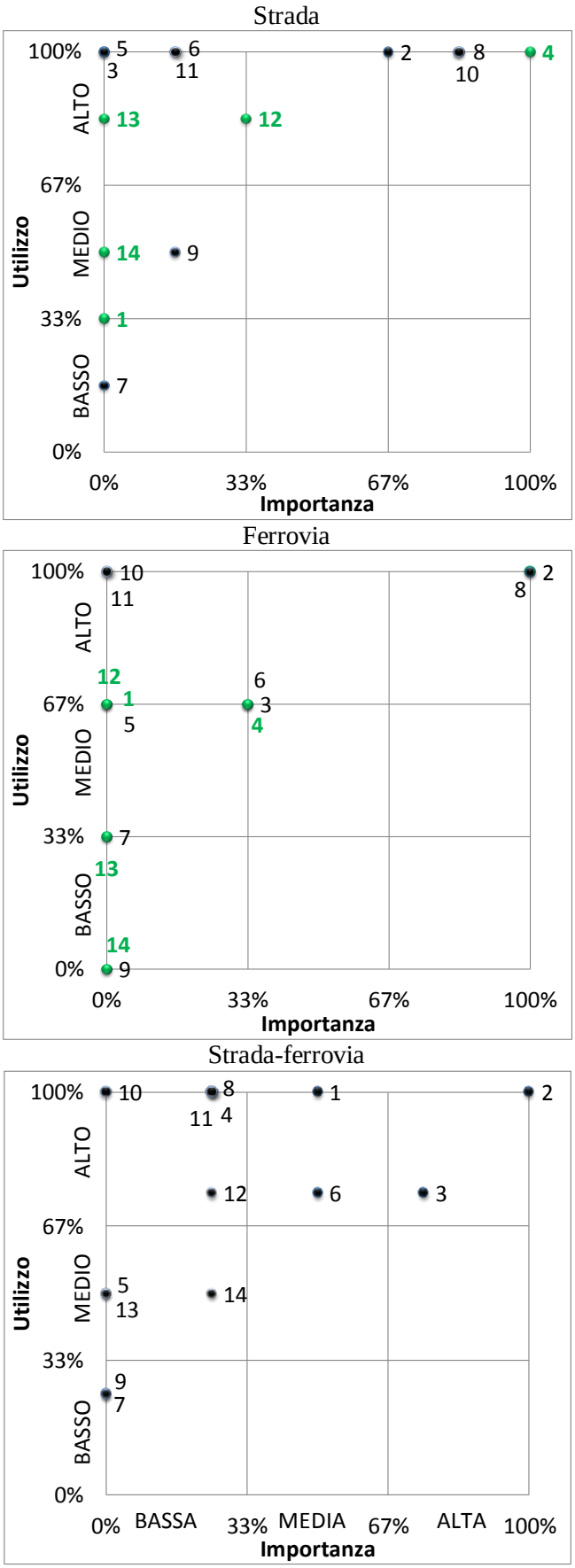
IMPATTO SULLA SICUREZZA DI FORNITURA PER AZIENDE POCO INTEGRATE		
12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	88%
11	Partnership	54%
9	Knowledge management	50%
10	Valutazione della conformità di sicurezza	50%
8	Segnalare incidenti e debolezze	27%
13	Riduzione della differenza di cultura tra aziende e partner	22%
6	Continuous improvement	15%
14	Focus sul cliente	6%
5	Aspetti soft	2%
1	Forza lavoro multidisciplinare	0%
2	Collaborazione tra dipendenti	0%
3	Integrità, lealtà dei dipendenti	0%
4	Sviluppo della consapevolezza interna sulla sicurezza	0%
7	Business continuity planning	0%

Per la sicurezza di fornitura risultano più importanti gli strumenti esterni sia per le aziende fortemente integrate (probabilità d'impatto degli strumenti esterni pari a 55% contro il 28% degli interni), sia per le aziende poco integrate (probabilità d'impatto degli strumenti esterni pari a 44% contro il 14% degli interni). Si può constatare che, per le aziende non integrate, 5 strumenti (tutti interni) sui 14 totali non hanno impatti sul ritardo al cliente finale.

6.2.3 Analisi in base al fattore ambito

Analisi utilizzo-importanza degli strumenti

In Figura 50 sono riportati i grafici di utilizzo/importanza per i tre diversi ambiti di cui un'azienda può occuparsi.



(1) Forza lavoro multidisciplinare

(2) Collaborazione tra dipendenti

(3) Integrità, lealtà dei dipendenti

(4) Sviluppo della consapevolezza interna sulla sicurezza

(5) Aspetti soft

(6) Continuous improvement

(7) Business continuity planning

(8) Segnalare incidenti e debolezze

(9) Knowledge management

(10) Valutazione della conformità di sicurezza

(11) Partnership

(12) Sviluppo della consapevolezza sulla sicurezza con i miei partner

(13) Riduzione della differenza di cultura tra aziende e partner

(14) Focus sul cliente

Figura 50: utilizzo/importanza-ambito

Tramite il fattore di contesto ambito è possibile spiegare l'utilizzo dei seguenti strumenti:

(1)	Strada		Ferrovia		Strada -ferrovia	
Forza lavoro multidisciplinare	Applicazione	33%	Applicazione	67%	Applicazione	100%
	Applicazione formale	33%	Applicazione formale	33%	Applicazione formale	100%

Come detto nel paragrafo 6.2.1, l'ambito è il fattore di contesto che spiega meglio l'utilizzo di una forza multidisciplinare.

Tutte le aziende che svolgono attività in ambito ferroviario (ad eccezione di Terminali Italia) utilizzano questo strumento (di cui 5 in modo formale e 1 in modo non formale). Il motivo è legato a due caratteristiche tipiche di questa struttura. Il primo è che l'organizzazione del lavoro all'interno di un terminal è strutturata in diverse mansioni operative numericamente superiori a quelle di un vettore stradale (controllo in ingresso della ILU, trasbordo, movimentazione interna, verifica dei carri, prova freno) da effettuare contestualmente, un esempio a tal proposito sono le mansioni di controllo, le quali prevedono una conoscenza ad ampio spettro sulle possibili anomalie da rilevare; in questo contesto non è pensabile avere operatori specializzati sulla singola operazione, questo comporterebbe uno spreco di risorse e rigidità nello svolgimento di tutti i processi. La seconda motivazione è che la concentrazione delle operazioni in un'unica area favorisce e aiuta una formazione multidisciplinare degli attori. Come dice Davide Muzio[55] *"in un terminal, grande o piccolo che sia, trattando una serie di operazioni, tutti devono sapere cosa avviene prima e cosa dopo ed avere perciò una competenza allargata"*.

Lo strumento è generalmente utilizzato in modo formale; solo TIMO lo applica in modo informale a causa delle sue esigue dimensioni. Le aziende che si occupano solamente della tratta stradale possono scegliere di avere dei dipendenti con competenze allargate oppure specializzate. La specializzazione degli autisti può avvenire in due modi: in base alla tipologia di ILU da trasportare (Marenzana) o alla tipologia di merce (BAS). L'unica azienda ad utilizzare lo strumento, è Hoyer che possiede autisti in grado di gestire ogni tipologia di merce e svolgere mansioni aggiuntive come ad esempio il

[55] Davide Muzio, Consigliere Delegato di TIMO

controllo e verifiche di conformità. Come dice Sabrina Robba[56] *"noi tendiamo ad avere autisti che siano in grado di gestire ogni tipologia di prodotto. […] L'autista non è solo colui che guida il camion ma è la persona che conosce il prodotto trasportato e quando va a ritirare o a consegnare la merce partecipa attivamente al carico o allo scarico […] insomma ha un ruolo molto più ampio rispetto ai tradizionali autisti"*.

Tutte le aziende che si occupano di entrambi gli ambiti utilizzano lo strumento, con particolare riferimento all'interfaccia con la ferrovia (gestione personale dentro il terminal).

(4)	**Strada**		**Ferrovia**		**Strada –ferrovia**	
Sviluppo della consapevolezza interna sulla sicurezza	Applicazione	100%	Applicazione	67%	Applicazione	100%
	Applicazione formale	100%	Applicazione formale	33%	Applicazione formale	100%

Oltre alla dimensione, il fattore causa ambito spiega l'utilizzo dello strumento 4. Le aziende che si interfacciano con la strada risultano più attente a tematiche di sicurezza sia di attacchi che di fornitura. Il motivo potrebbe risiedere nel fatto che queste lavorano a stretto contatto con i clienti i quali richiedono il rispetto di determinati standard. Risalendo nella filiera fino ai terminal, questa consapevolezza sulle tematiche di sicurezza si affievolisce. Oltretutto i rischi di incorrere in una disruption in un terminal (considerata la concentrazione di tutte le attività in un unico sito dei G) sono meno variabili rispetto a quelli presenti in ambito stradale.

(8)	**Strada**		**Ferrovia**		**Strada –ferrovia**	
Segnalare incidenti e debolezze	Applicazione	100%	Applicazione	100%	Applicazione	100%
	Applicazione formale	83%	Applicazione formale	33%	Applicazione formale	0%

Seppur questo strumento è utilizzato dall'intero campione di aziende intervistate, risulta evidente come per le imprese con interfaccia stradale vi sia un maggior impegno nella formalizzazione dello strumento; questo perché in ambito stradale esiste una più elevata variabilità dei rischi come spiegato per lo strumento 8. Questo spinge le aziende con interfaccia stradale ad instituire uno strumento formale che monitori anche i near misses per poter così imparare e talvolta migliorare le procedure esistenti o ridurre al minimo le

[56] Managing Director di HOYER Italia S.r.l. e di HOYER Svizzera SA e responsabile della sicurezza, ambiente e qualità di tutto il gruppo HOYER

principali cause degli incidenti. Come testimoniato da Sabrina Robba[57] *"quando accadono quelli che noi chiamiamo main incident, noi abbiamo un sistema di incident investigation (che è un form da compilare con su tutte le informazioni relative e, dove vengono identificate, anche le azioni correttive e preventive per evitare che l'incidente possa accadere ancora), ma può capitare che per alcuni near misses venga considerata l'idea di fare un'incident investigation da cui poi scaturiscono una serie di azioni correttive, tra le quali una parte preponderante riguarda piani di training è […] L'autista riporta verbalmente la situazione di pericolo o di quasi incidente ed il responsabile locale della sicurezza compila il formulario dei near misses."*

(12)	**Strada**		**Ferrovia**		**Strada –ferrovia**	
Sviluppo della consapevolezza sulla sicurezza con i partner	Applicazione	83%	Applicazione	67%	Applicazione	75%
	Applicazione formale	50%	Applicazione formale	33%	Applicazione formale	75%

Oltre alla dimensione, anche l'ambito influisce sull'utilizzo. Lo strumento è applicato da quasi tutte le aziende che si occupano della tratta su strada (5 su 6) ed è rivolto sempre ai vettori stradali. Quasi tutti gli MTO (M e MV) lo applicano, perché hanno maggiore interesse nell'educazione dei propri partner (siccome il cliente finale attribuisce a loro la responsabilità di eventuali cattive prestazioni). Solo nel caso di BAS non viene applicato perché è l'unica ad avere esclusivamente padroncini interni. Riportiamo in seguito la testimonianza di Gianfranco Brillante[58] relativa ad un MTO puro (M) che si è occupato in prima persona della formazione sulle tematiche di sicurezza dei propri partner: "*Abbiamo fatto intervenire una società tedesca specializzata nella sicurezza stradale. Abbiamo invitato i nostri padroncini e gli abbiamo fatto fare un corso di formazione su come si fa a legare la merce, a seconda del tipo di merce. Abbiamo fatto vedere prima come si deve legare, e poi quali sono gli effetti di un'operazione fatta bene o male. C'è stata prima una formazione teorica nella quale sono stati visionati dei filmati e delle slide, e poi una prova pratica su piazzale per capire cosa succede".*

Dal lato ferrovia, 2 gestori di terminal su 3 (escluso Terminali Italia) applicano lo strumento, seppur con una modalità differente rispetto agli MTO; infatti, un gestore di

[57] Managing Director di HOYER Italia S.r.l. e di HOYER Svizzera SA e responsabile della sicurezza, ambiente e qualità di tutto il gruppo HOYER

[58] Gianfranco Brillante, Direttore di filiale Fercam

terminal (G) si limita a dettare ai partner di filiera le procedure da adottare. Differente è la posizione di Hupac che, grazie al ruolo che ricopre nella filiera (GO) e la sua dimensione, è in grado di proporsi come promotore delle iniziative di formazione continua sulla sicurezza ed educatore dei partner della filiera; non si limita quindi a stilare un elenco di requisiti da rispettare. Il fatto che questo strumento sia più utilizzato da chi si occupa del lato strada, è confermato anche dall'importanza che essi associano allo strumento: infatti, tra gli MTO, 2 su 6 hanno detto che è importante mentre lato ferrovia 0 aziende su 3 hanno affermato ciò. Seppure siano percentuali piuttosto basse, a causa della generale scarsa importanza che le aziende riconoscono negli strumenti esterni, si avverte una discreta differenza.

(13)	**Strada**		**Ferrovia**		**Strada –ferrovia**	
Riduzione della differenza di cultura tra azienda e partner	Applicazione	83%	Applicazione	33%	Applicazione	50%
	Applicazione formale	50%	Applicazione formale	33%	Applicazione formale	25%

Oltre alla dimensione, anche l'ambito influisce sull'utilizzo di questo strumento. Analogamente allo sviluppo della consapevolezza sulla sicurezza con i partner, sono gli MTO (M+MV) i principali promotori di un processo di riduzione della differenza di cultura tra azienda e partner. Le iniziative vengono intraprese in prima persona dagli MTO quasi sempre in modo formale (4 casi su 5) attraverso incontri, riunioni e convention focalizzate sulla sicurezza ai quali sono invitati i propri partner. Invece i gestori dei terminal (G) generalmente non sono mai gli organizzatori e promotori di questo tipo di iniziative. Infatti, come detto precedentemente a proposito dello strumento 12, l'elemento differenziale è la responsabilità sulla sicurezza e sono gli MTO che avendo un rapporto diretto con il cliente finale vengono responsabilizzati in questo senso.

Lato ferrovia l'unico che lo applica è Hupac (GO) per lo stesso motivo visto per lo strumento 12. Come dice Sergio Crespi[59] *"Tutti gli anni facciamo delle customer convention parlando della sicurezza a 360 gradi, oltre che della parte commerciale, piuttosto che del servizio alla clientela, della qualità, della puntualità dei treni eccetera. Queste iniziative ci servono per migliorare la collaborazione e l'integrazione con i*

[59] Sergio Crespi, Direttore Generale del terminal intermodale di Busto Arsizio/Gallarate

partner e la loro fidelizzazione. Sono iniziative rivolte sia ai nostri clienti che ai nostri fornitori che servono per migliorare la qualità della partnership".

(14)	Strada		Ferrovia		Strada –ferrovia	
Focus sul cliente	Applicazione	50%	Applicazione	0%	Applicazione	25%
	Applicazione formale	0%	Applicazione formale	0%	Applicazione formale	0%

Le uniche aziende ad avere un'ottica di filiera sono quelle che si interfacciano con il cliente finale. A testimonianza di ciò tutti gli MTO puri (M) applicano lo strumento. Queste aziende però devo avere anche altre caratteristiche: devono essere grandi o integrate (per le spiegazioni si rimanda alle relative sezioni). Un MTO piccola, infatti, non può esercitare un'influenza tale da far applicare questo strumento: ad esempio, in riferimento a Bas (MV piccolo), Alessandro Negri[60]: afferma che *"essendo il punto di riferimento per il cliente, spesso abbiamo a che fare con reclami per problematiche non causate direttamente da noi. Per esempio quando un treno si ferma, non abbiamo alcun margine per intervenire, ma il cliente si rifà su di noi. Ad oggi, per un'azienda come la nostra, è questo il vero limite del trasporto intermodale"*.

Viceversa aziende grandi e integrate ma che non vedono il cliente finale non riescono a proporre un approccio di filiera: in riferimento a Hupac (GO, grande e completamente integrata sulla ferrovia), Sergio Crespi[61] afferma che *"non sappiamo neanche dove sarà la consegna finale dei treni che componiamo. Non fa parte del nostro business e non è di nostro interesse"*.

Analisi importanza dei fattori causa

In Figura 51 si riportano i grafici relativi all'importanza dei fattori causa per la sicurezza da attacchi e quella di fornitura per aziende che si occupano rispettivamente solo della tratta su strada, solo dell'interfaccia con la ferrovia o di entrambe.

[60] Alessandro Negri, Manager Operations di Bas Logistic

[61] Sergio Crespi, Direttore Generale del terminal intermodale di Busto Arsizio/Gallarate

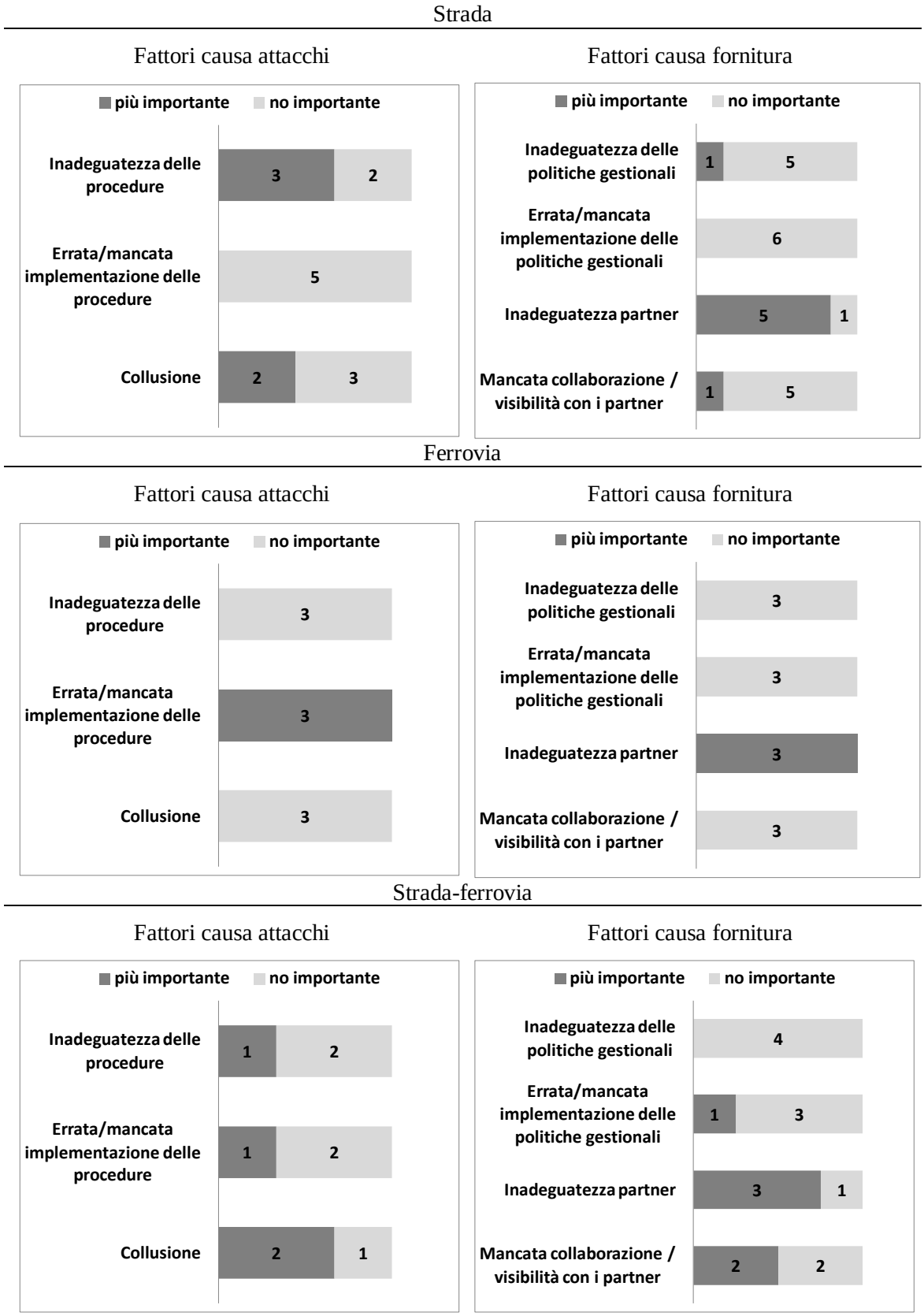


Figura 51: importanza dei fattori causa-ambito

Si evidenzia come, dal punto di vista della sicurezza attacchi, la causa principale di una cattiva prestazione sia discordante tra i due ambiti. Tutti gli operatori dell'ambito

ferrovia individuano l'errata /mancata implementazione delle procedure come la causa principale; questo probabilmente perché rispetto ai vettori stradali (tra cui nessuno ne ha segnalato l'importanza) i gestori di un terminal hanno un numero maggiore di operazioni da effettuare. Chi si interfaccia con la strada ha invece evidenziato la collusione come prima causa (per strada-ferrovia) e seconda causa (solo per la strada) di furti e manipolazioni. Probabilmente perché è più facile organizzare un furto su strada piuttosto che in un'area video sorvegliata come quella di un terminal. Nello specifico chi si interfaccia con entrambi gli ambiti evidenzia come il fattore causa principale sia la collusione perché è proprio durante il cambio di modalità di trasporto che si possono verificare episodi collusivi tra operatori del terminal e autisti.

L'inadeguatezza delle procedure è il principale fattore causa per chi si occupa solo della tratta su strada, con un peso di 3 su 5.

Riguardo la sicurezza di fornitura tutti gli ambiti sono in accordo sul fatto che l'inadeguatezza del partner è la causa principale. L'impatto del ritardo del trazionista si ripercuote sia su chi gli è a stretto contatto (G e GO) sia sugli altri anelli più distanti della supply chain. Questo denota il fatto che per assorbire totalmente il ritardo del trazionista non siano sufficienti gli sforzi congiunti degli altri operatori ferroviari (G e GO) ma l'effetto si ripercuote inevitabilmente anche sugli operatori stradali. Questo evidenzia di quanto le prestazioni di filiera siano legate strettamente alle prestazioni di ogni singolo anello.

Si nota come, per chi si occupa della tratta stradale, la mancanza di collaborazione e di visibilità con il partner sia avvertito come un ulteriore problema dati i numerosi passaggi di informazione.

Analisi impatto degli strumenti sulla sicurezza

La Tabella 56, la Tabella 57 e la Tabella 58 riportano i 14 strumenti ordinati in base all'impatto che hanno sulla sicurezza da attacchi per le aziende rispettivamente con interfaccia stradale, ferroviaria e strada-ferrovia.

Tabella 56: Aziende con interfaccia stradale

IMPATTO SULLA SICUREZZA DA ATTACCHI PER AZIENDE CON INTERFACCIA STRADA		
3	Integrità, lealtà dei dipendenti	70%
10	Valutazione della conformità di sicurezza	57%
6	Continuous improvement	54%
11	Partnership	52%
13	Riduzione della differenza di cultura tra aziende e partner	50%
5	Aspetti soft	50%
9	Knowledge management	50%
2	Collaborazione tra dipendenti	48%
8	Segnalare incidenti e debolezze	45%
4	Sviluppo della consapevolezza interna sulla sicurezza	40%
12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	35%
14	Focus sul cliente	35%
1	Forza lavoro multidisciplinare	26%
7	Business continuity planning	0%

Tabella 57: Aziende con interfaccia ferroviaria

IMPATTO SULLA SICUREZZA DA ATTACCHI PER AZIENDE CON INTERFACCIA FERROVIA		
6	Continuous improvement	86%
2	Collaborazione tra dipendenti	69%
4	Sviluppo della consapevolezza interna sulla sicurezza	64%
1	Forza lavoro multidisciplinare	57%
8	Segnalare incidenti e debolezze	57%
5	Aspetti soft	50%
11	Partnership	50%
3	Integrità, lealtà dei dipendenti	46%
10	Valutazione della conformità di sicurezza	40%
12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	32%
13	Riduzione della differenza di cultura tra aziende e partner	21%
7	Business continuity planning	0%
9	Knowledge management	0%
14	Focus sul cliente	0%

Tabella 58: Aziende con interfaccia strada-ferrovia

IMPATTO SULLA SICUREZZA DA ATTACCHI PER AZIENDE CON INTERFACCIA STRADA-FERROVIA		
11	Partnership	100%
5	Aspetti soft	80%
13	Riduzione della differenza di cultura tra aziende e partner	72%
10	Valutazione della conformità di sicurezza	69%
8	Segnalare incidenti e debolezze	58%
6	Continuous improvement	53%
2	Collaborazione tra dipendenti	52%
12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	44%
1	Forza lavoro multidisciplinare	41%
4	Sviluppo della consapevolezza interna sulla sicurezza	41%
3	Integrità, lealtà dei dipendenti	40%
7	Business continuity planning	40%
9	Knowledge management	28%
14	Focus sul cliente	-33%

È interessante notare come la probabilità di impatto degli strumenti interni ed esterni sulla sicurezza da attacchi cambi totalmente passando dall'ambito stradale a quello ferroviario. Per le aziende che si interfacciano solo con la strada la probabilità d'impatto degli strumenti esterni è più elevata rispetto a quelli interni (49% contro 43%); per le aziende che hanno la doppia interfaccia la percentuale d'impatto è pressoché uguale (50% per gli interni contro il 51% per gli esterni); mentre per chi si occupa

esclusivamente dell'ambito ferroviario vi è una netta differenza a favore degli strumenti interni (47% interni contro 29% degli esterni). Questo dato conferma le teorie precedentemente descritte: chi si occupa di strada (M e MV) hanno una visione più ampia e conoscono l'impatto che i loro partner hanno sulla prestazione finale di sicurezza da attacchi (il quale poi si lamenterà con gli MTO stessi) per cui cerca di adottare strumenti che coinvolgono i processi dei loro partner in ottica di miglioramento delle prestazioni di filiera. Per quanto riguarda l'ambito ferroviario invece, i gestori del terminal (G) e gli operatori commerciali logistici (GO), si preoccupano maggiormente del miglioramento intra-aziendale e hanno delle lacune per quanto riguarda l'applicazione di strumenti a più ampio spettro nella filiera.

La Tabella 59, Tabella 60 e Tabella 61 riportano i 14 strumenti ordinati in base all'impatto che hanno sulla sicurezza da attacchi per le aziende rispettivamente con interfaccia stradale, ferroviaria e strada-ferrovia.

Tabella 59: Aziende con interfaccia stradale

IMPATTO SULLA SICUREZZA DI FORNITURA PER AZIENDE CON INTERFACCIA STRADA		
12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	88%
11	Partnership	54%
9	Knowledge management	50%
10	Valutazione della conformità di sicurezza	50%
8	Segnalare incidenti e debolezze	27%
13	Riduzione della differenza di cultura tra aziende e partner	22%
6	Continuous improvement	15%
14	Focus sul cliente	6%
5	Aspetti soft	2%
1	Forza lavoro multidisciplinare	0%
2	Collaborazione tra dipendenti	0%
3	Integrità, lealtà dei dipendenti	0%
4	Sviluppo della consapevolezza interna sulla sicurezza	0%
7	Business continuity planning	0%

Tabella 60: Aziende con interfaccia ferroviaria

IMPATTO SULLA SICUREZZA DI FORNITURA PER AZIENDE CON INTERFACCIA FERROVIA		
13	Riduzione della differenza di cultura tra aziende e partner	100%
11	Partnership	50%
12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	50%
1	Forza lavoro multidisciplinare	0%
2	Collaborazione tra dipendenti	0%
3	Integrità, lealtà dei dipendenti	0%
4	Sviluppo della consapevolezza interna sulla sicurezza	0%
5	Aspetti soft	0%
6	Continuous improvement	0%
7	Business continuity planning	0%
8	Segnalare incidenti e debolezze	0%
9	Knowledge management	0%
10	Valutazione della conformità di sicurezza	0%
14	Focus sul cliente	0%

Tabella 61: Aziende con interfaccia strada-ferrovia

IMPATTO SULLA SICUREZZA DI FORNITURA PER AZIENDE CON INTERFACCIA STRADA-FERROVIA		
11	Partnership	88%
10	Valutazione della conformità di sicurezza	58%
13	Riduzione della differenza di cultura tra aziende e partner	42%
12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	33%
14	Focus sul cliente	33%
2	Collaborazione tra dipendenti	25%
8	Segnalare incidenti e debolezze	25%
1	Forza lavoro multidisciplinare	17%
4	Sviluppo della consapevolezza interna sulla sicurezza	17%
9	Knowledge management	17%
3	Integrità, lealtà dei dipendenti	11%
6	Continuous improvement	11%
5	Aspetti soft	8%
7	Business continuity planning	0%

Per quanto riguarda la sicurezza di fornitura la probabilità di impatto degli strumenti interni ed esterni diminusce passando dall'ambito stradale a quello ferroviario. Per le aziende che si interfacciano solo con la strada la probabilità d'impatto degli strumenti esterni è più elevata rispetto a quelli interni (55% contro 33%); stesso discorso vale per le aziende che hanno la doppia interfaccia (51% per gli esterni contro il 19% per gli interni); per chi si occupa esclusivamente dell'ambito ferroviario vi è l'applicazione dei

soli strumenti esterni (40%). Questo dato sicuramente ci fornisce l'indicazione che gli strumenti esterni sono percepiti come più importanti e con più impatti in relazione alla sicurezza di fornitura per tutte le categorie di azienda. Un approfondimento merita l'ambito ferroviario per il quale risultano impattare sul ritardo al cliente finale solo 3 strumenti (tutti esterni). Il forte impatto che rivestono gli strumenti esterni nella prestazione di sicurezza di fornitura rimarca ancora una volta il fatto che in una supply chain, per raggiungere buone prestazioni, è molto importante l'integrazione dei processi dei differenti partner.

6.2.4 Sintesi dell'analisi sui fattori di contesto

Dalle analisi inerenti ai diversi fattori di contesto si denota, come si poteva presumere, che in genere le aziende di dimensioni più elevate sono spinte verso un utilizzo ed una formalizzazione degli strumenti maggiore. Questo fenomeno è dovuto alla maggiore complessità interna di queste aziende per le quali risulta difficile poter raggiungere obiettivi di sicurezza senza l'utilizzo formale degli strumenti proposti. Un ulteriore motivo di questa discrepanza tra piccole e grandi aziende risiede nel fatto che la maggior dimensione, con conseguente maggior strutturazione, maggior volume d'affari e maggior potere contrattuale, pone le grandi aziende in una posizione privilegiata nell'applicare gli strumenti proposti.

Per quanto riguarda l'integrazione invece, non c'è una così netta differenza nell'utilizzo degli strumenti proposti. In generale le aziende più integrate sono di grandi dimensioni, possono quindi applicare molti strumenti e in modo formale, è altrettanto vero che però esistono numerose imprese di grandi dimensioni non integrate che possono fare altrettanto. Come spiegato l'integrazione è un fattore discriminante soltanto per due strumenti: la forza lavoro multidisciplinare (anche se spiegata meglio dall'ambito) e il BCP.

Passando al fattore di contesto ambito abbiamo notato come tutti quegli strumenti esterni legati alle prestazioni di filiera vengano maggiormente implementati dalle aziende stradali. Come descritto in precedenza la motivazione che spinge questa tipologia di aziende ad applicare questi strumenti è la responsabilità sulle prestazione che detengono di fronte al cliente finale essendo la loro interfaccia; sono quindi queste aziende che hanno sviluppato maggiormente il senso di appartenenza ad un'unica filiera e si impegnano nel ridurre le differenze culturali, sviluppare le competenze e la consapevolezza sulle tematiche di sicurezza così da raggiungere elevati target

prestazionali ed acquisire credibilità e fiducia verso i clienti industriali. Si nota inoltre un'altra differenza tra le aziende appartenenti ad ambiti diversi. Da un lato le aziende con interfaccia ferroviaria hanno la necessità di impiegare una forza lavoro multidisciplinare dato l'elevato numero di mansioni operative svolte all'interno del terminal intermodale (basti pensare ai diversi controlli da effettuare contestualmente all'arrivo e al trasbordo delle ILU); dall'altro le aziende che lavorano in ambito stradale applicano in modo più strutturato e formale gli strumenti legati allo sviluppo delle competenze di sicurezza e alla segnalazione di incidenti. Questa tendenza è dovuta al fatto che in ambito stradale esiste una maggior variabilità dei rischi di incorrere in una disruption rispetto all'ambito ferroviario (in un terminal tutte le attività sono svolte in un unico sito, mentre una società di trasporti su gomma per sua stessa natura svolge le sue attività in siti differenti ed è quindi esposta a maggiori rischi).

6.3 Analisi incrociata

In questo paragrafo ultimeremo le nostre analisi proponendo delle check-list di strumenti in funzione dei differenti fattori di contesto. Siccome queste check-list sono derivate da considerazioni ed analisi effettuate su aziende operanti nel trasporto intermodale, l'applicazione di queste, consentono di raggiungere prestazioni di sicurezza in linea con il settore.

Per poter creare le check-list dobbiamo procedere con un'analisi incrociata. Dobbiamo cioè confrontare, per ogni strumento, la forza dei vari fattori di contesto nello spiegare l'utilizzo (o in alcuni casi il tipo di utilizzo) dello strumento analizzato. Per ogni strumento quindi abbiamo confrontato le percentuali di utilizzo esposte nelle sezioni precedenti integrandole con le informazioni recepite durante le interviste per poter infine capire quale fattore di contesto spiega l'utilizzo (o l'utilizzo formale) di ogni specifico strumento.

Abbiamo schematizzato in Tabella 62 il risultato. Esso è una sintesi e un'astrazione di tutte le analisi precedentemente effettuate sul campione d'aziende intervistate. Esprime quindi quali sono i fattori di contesto che discriminano i vari strumenti sull'utilizzo e sul tipo di utilizzo. Abbiamo collocato la lettera opportuna in corrispondenza della caratteristica che giustifica il maggior utilizzo dello strumento; nel caso uno strumento abbia più di un fattore di contesto discriminante abbiamo individuato, tramite i dati discussi nelle precedenti analisi e considerazioni di tipo qualitativo, quello principale.

Riteniamo che per due strumenti (4 e 14) i fattori discriminanti dimensione e ambito siano di uguale importanza.

Legenda:

A: il fattore di contesto è il principale discriminante per quanto riguarda l'applicazione dello strumento

A: il fattore di contesto spiega l'applicazione dello strumento ma non è il principale discriminante

F: il fattore di contesto è il principale discriminante per quanto riguarda l'utilizzo formale dello strumento

F: il fattore di contesto spiega l'utilizzo formale dello strumento ma non è il principale discriminante

Tabella 62: tabella riassuntiva strumenti-fattori di contesto discriminanti

	Strumenti	Dimensione		Integrazione		Ambito	
		Grande	Piccola	Alta	Bassa	Strada	Ferrovia
1	Forza lavoro multidisciplinare	A		A			**A**
2	Collaborazione tra dipendenti	**F**					
3	Integrità, lealtà dei dipendenti	**F**					
4	Sviluppo della consapevolezza interna sulla sicurezza	**F**				**F**	
5	Aspetti soft	**F**					
6	Continuous improvement	**F**					
7	Business continuity planning	**A**		**A**			
8	Segnalare incidenti e debolezze					**F**	
9	Knowledge management	**A**					
10	Valutazione della conformità di sicurezza	**F**					
11	Partnership						
12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	F				**A**	
13	Riduzione della differenza di cultura tra aziende e partner	F				**A**	
14	Focus sul cliente	**A**				**A**	

Di seguito spiegheremo brevemente le motivazioni che hanno portato alla corretta compilazione della Tabella 62, per approfondimenti in merito rimandiamo al paragrafo 6.2.

Forza lavoro multidisciplinare (1): come analizzato precedentemente è applicato maggiormente dalle aziende grandi, da quelle più integrate e da quelle che si occupano dell'ambito ferroviario. Riteniamo che però sia proprio quest'ultimo fattore di contesto

a spiegare maggiormente l'utilizzo dello strumento 1 dato il numero maggiore di differenti mansioni operative rispetto a quelle di un vettore stradale.

Collaborazione tra dipendenti (2): le aziende più grandi tendono ad utilizzare in modo più formale lo strumento data la loro maggiore complessità interna

Integrità, lealtà dei dipendenti (3): si nota una maggior formalità d'applicazione per le aziende con dimensioni più elevate; il motivo è legato all'elevato numero di dipendenti che impedisce uno stretto contatto personale che invece si instaura nelle piccole aziende.

Sviluppo della consapevolezza interna sulla sicurezza (4): si nota sia applicato formalmente sia dalle aziende di grandi dimensioni sia da quelle che si occupano dell'ambito stradale. Riteniamo che la complessità organizzativa (e quindi la dimensione), il contatto diretto con i clienti che richiedono il rispetto di determinati standard e l'alta variabilità dei rischi presenti in ambito stradale concorrano in egual misura all'applicazione formale di questo strumento.

Aspetti soft (5): la maggior strutturazione organizzativa gioca un ruolo fondamentale nell'implementazione di un programma completo di corporate governance; le piccole aziende utilizzano comunque lo strumento seppur in modo informale.

Continuous improvement (6): le aziende di dimensioni più elevate tendono a standardizzare i processi di miglioramento continuo, mentre per le piccole ci si affida di più alla discrezione del singolo individuo e al rapporto personale instaurato tra operatore e manager.

Business Continuity Planning (7): è strettamente legato alla possibilità di influenzare il trazionista ferroviario; riteniamo quindi che la grossa dimensione (potere contrattuale) e l'alta integrazione (vicinanza all'operatore ferroviario e possibilità di organizzare un trasporto alternativo) concorrano in ugual modo verso l'applicazione dello strumento.

Segnalare incidenti e debolezze (8): è applicato indistintamente da tutte le aziende intervistate, ma è presente uno sforzo maggiore per quanto riguarda la sua formalizzazione da parte delle aziende che si occupano del trasporto su strada (data la maggior variabilità dei rischi).

Knowledge management (9): seppur utilizzato nella maggior parte dei casi in modo informale, lo strumento è applicato maggiormente dalle aziende di grandi dimensioni che presentano una varietà di casistiche e un numero di persone tale da poter giustificare da un lato l'investimento in un software di knowledge management, e dell'altro il tempo dedicato alla codifica delle esperienze.

Valutazione della conformità di sicurezza (10): è utilizzato dalla totalità del campione di aziende ma si è notato che quelle di grandi dimensioni tendono ad adottare un meccanismo formale per la valutazione della sicurezza dei processi interni e dei propri partner, mentre quelle di piccole dimensioni si limitano ad ottenere le certificazioni necessarie.

Partnership (11): viene applicata in modo formale da tutte le aziende intervistate

Sviluppo della consapevolezza sulla sicurezza con i propri partner (12): riteniamo che l'utilizzo di questo strumento sia discriminato in base a due fattori di contesto: dimensione e ambito. Da un lato la focal company della filiera (in genere di grandi dimensioni) ha la necessità di sviluppare, tramite uno strumento formale, le competenze e la consapevolezza sulle tematiche di sicurezza dei partner, spesso più piccoli e meno strutturati. Dall'altro lato quasi tutti gli MTO (M e MV) hanno maggiore interesse nell'educazione dei propri partner, siccome il cliente finale attribuisce loro la responsabilità di eventuali cattive prestazioni.

Riduzione della differenza di cultura tra aziende e partner (13): come per lo strumento 12, riteniamo che l'utilizzo sia discriminato in base ai fattori di contesto dimensione e ambito. Le grandi aziende sono le sole ad avere la capacità e i mezzi per poter applicare in modo formale questo strumento e contribuire direttamente al miglioramento della prestazione finale di sicurezza. Il principale fattore discriminante è invece l'ambito: chi appartiene a quello stradale si interfaccia sempre con il cliente finale ed è da questo responsabilizzato in termini di sicurezza, ha così l'obbligo di migliorare le prestazioni di filiera anche tramite l'utilizzo dello strumento in questione.

Focus sul cliente (14): affinché venga applicato, seppur sempre in maniera informale, devono coesistere due caratteristiche: la grande dimensione e l'appartenenza all'ambito stradale. Il motivo della prima è che solo aziende di una certa dimensione hanno la possibilità di esercitare un'influenza sulle altre per creare un processo di filiera orientato al cliente finale. D'altro canto le uniche che si interfacciano con il cliente, e sono quindi spinte ad applicare lo strumento, sono quelle appartenenti all'ambito stradale.

Intrecciando i tre fattori di contesto si individuano 8 cluster presentati in Tabella 63.

Tabella 63: classificazione aziende intermodali

		AMBITO			
		Strada		Ferrovia	
INTEGRAZIONE		Alta	Bassa	Alta	Bassa
DIMENSIONE	Grande	A	C	E	G
	Piccola	B	D	F	H

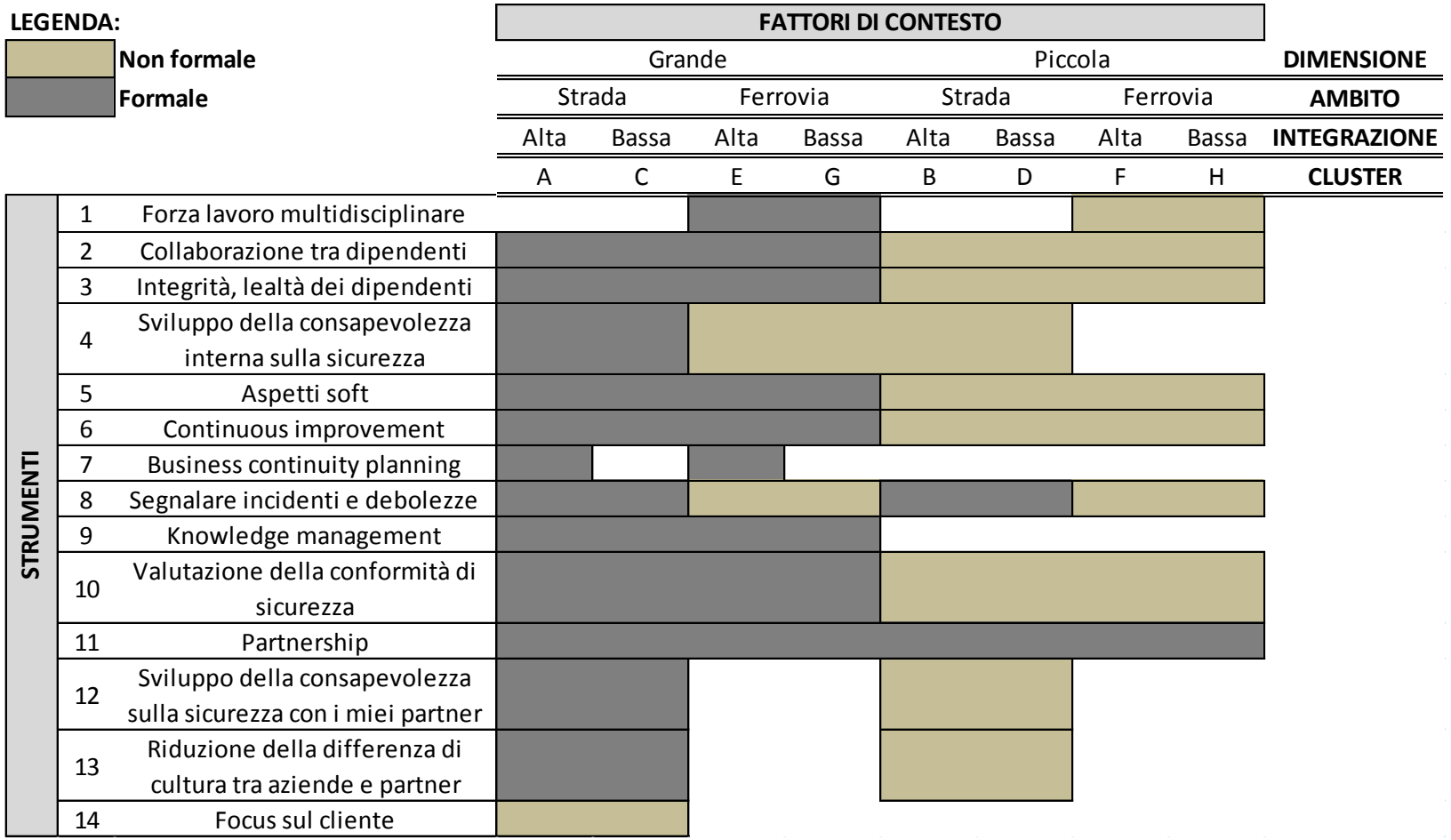
Partendo dalle informazioni presenti in Tabella 62, con riferimento alla classificazione di Tabella 63, abbiamo potuto creare 8 differenti check-list di strumenti ognuna associata ad un cluster. Questo ci consentirà di evidenziare quali strumenti le aziende adottano in funzione dei loro specifici fattori di contesto e rispondere così alla domanda di ricerca n° 2. Si sottolinea il fatto che le check-list non derivano dall'analisi puntuale delle frequenze di utilizzo di ogni azienda bensì sono il frutto di un ragionamento induttivo a partire dalle analisi sui fattori di contesto riassunte in Tabella 62.

Di seguito è riportato in Tabella 64 l'analisi incrociata tra gli strumenti proposti e i fattori di contesto. Da questo schema si possono distinguere due tipologie di strumenti:

- comuni, ovvero strumenti utilizzati da tutti i cluster;
- caratteristici, ovvero strumenti utilizzati dal cluster in questione e non da tutti gli altri cluster.

La tabella inoltre evidenzia la differente modalità di utilizzo degli strumenti in relazione allo specifico cluster di appartenenza.

Tabella 64: assegnazione strumenti al cluster



A partire dalla Tabella 64 abbiamo stilato le check-list riferite agli 8 cluster.

Tabella 65:check-list del cluster A

Check-list strumenti per cluster A		
Comuni	2	Collaborazione tra dipendenti
	3	Integrità, lealtà dei dipendenti
	5	Aspetti soft
	6	Continuous improvement
	8	Segnalare incidenti e debolezze
	10	Valutazione della conformità di sicurezza
	11	Partnership
Caratteristici	**4**	**Sviluppo della consapevolezza interna sulla sicurezza**
	7	**Business continuity planning**
	9 (n.f.)	**Knowledge management**
	12	**Sviluppo della consapevolezza sulla sicurezza con i miei partner**
	13	**Riduzione della differenza di cultura tra aziende e partner**
	14 (n.f.)	**Focus sul cliente**
Non utilizzati	1	Forza lavoro multidisciplinare

Il primo cluster è caratterizzato da:

- Dimensione grande
- Integrazione alta
- Ambito stradale

Questa tipologia di azienda ha la necessità e la struttura per utilizzare molti degli strumenti proposti per raggiungere buone prestazioni di sicurezza data la sua elevata complessità ed eterogeneità interna. Appartenendo inoltre all'ambito stradale ha una sensibilità particolare per quegli strumenti, come il 12, 13 e 14, che consentono di creare un senso di appartenenza alla filiera per tutti i nodi di quest'ultima. È evidenziato in Tabella 65 come lo strumento 9 sia applicato in modo informale perché non strettamente legato al settore intermodale come descritto in precedenza. Questo però, come schematizzato nelle Tabella 50, Tabella 54 e Tabella 59, è il terzo strumento che impatta maggiormente sulla sicurezza di fornitura per cui la sua applicazione formale potrebbe portare notevoli benefici. Esempi in questa direzione sono rappresentati in Tabella 73.

Si nota infine come solo la forza lavoro multidisciplinare sia l'unico strumento non utilizzato perché, come visto in precedenza, è utile principalmente in ambito ferroviario.

Tabella 66: check-list del cluster B

Check-list strumenti per cluster B		
Comuni	2 (n.f.)	Collaborazione tra dipendenti
	3 (n.f.)	Integrità, lealtà dei dipendenti
	5 (n.f.)	Aspetti soft
	6 (n.f.)	Continuous improvement
	8	Segnalare incidenti e debolezze
	10 (n.f.)	Valutazione della conformità di sicurezza
	11	Partnership
Caratteristici	**4 (n.f.)**	**Sviluppo della consapevolezza interna sulla sicurezza**
	12 (n.f.)	**Sviluppo della consapevolezza sulla sicurezza con i miei partner**
	13 (n.f.)	**Riduzione della differenza di cultura tra aziende e partner**
Non utilizzati	1	Forza multidisciplinare
	7	Business continuity planning
	9	Knowledge management
	14	Focus sul cliente

Il secondo cluster è caratterizzato da:

- Dimensione piccola
- Integrazione alta
- Ambito stradale

Si nota come, diminuendo le dimensioni, le aziende non applichino strumenti come il 7, il 9 e il 14 e abbandonino un utilizzo formale della maggior parte degli strumenti comuni. Il motivo risiede nel fatto che per un'azienda piccola, composta quindi da poche persone, è più semplice organizzare team (2), accogliere proposte dal basso (6), motivare gli operatori sulla lealtà verso l'azienda (3) senza l'ausilio di software particolari o processi standardizzati e formali. Come si può notare in Figura 46, Figura 48 e Figura 50 gli strumenti ritenuti più importanti sono il 2, l'8 e il 4. Questo perché per un'azienda piccola e integrata che si occupa del di trasporto su strada questi tre strumenti (anche applicati in modo informale) consentono di raggiungere buone prestazioni di sicurezza da attacchi impattando sui fattori causa più importanti (cioè errata/mancata implementazione delle procedure e inadeguatezza delle stesse). Per migliorare la sicurezza di fornitura, per la quale si identifica come fattore causa principale l'inadeguatezza del partner, le aziende di questo cluster applicano strumenti come il 12 e il 13; non si ha però la grandezza tale per farlo in modo strutturato e formale.

Tabella 67: check-list del cluster C

Check-list strumenti per cluster C		
Comuni	2	Collaborazione tra dipendenti
	3	Integrità, lealtà dei dipendenti
	5	Aspetti soft
	6	Continuous improvement
	8	Segnalare incidenti e debolezze
	10	Valutazione della conformità di sicurezza
	11	Partnership
Caratteristici	**4**	**Sviluppo della consapevolezza interna sulla sicurezza**
	9 (n.f.)	**Knowledge management**
	12	**Sviluppo della consapevolezza sulla sicurezza con i miei partner**
	13	**Riduzione della differenza di cultura tra aziende e partner**
	14 (n.f.)	**Focus sul cliente**
Non utilizzati	1	Forza multidisciplinare
	7	Business continuity planning

Il terzo cluster è caratterizzato da:

- Dimensione grande
- Integrazione bassa
- Ambito stradale

La bassa integrazione non permette di utilizzare lo strumento 7, questo è dovuto all'impossibilità di poter influenzare il trazionista. Lo strumento 1 non viene in genere implementato tranne in casi particolari (alta varietà di prodotti pericolosi) come testimonia il caso Hoyer Tabella 73; sempre dalla stessa tabella si evince come queste tipologie di aziende applichino in modo innovativo gli strumenti 4, 6, 8, 9 e 14. Questo dimostra un'attenzione particolare per quegli strumenti (4, 6, 8) ritenuti più importanti. È da notare come però questi strumenti non impattino molto sulla sicurezza di fornitura, mentre per quanto riguarda la sicurezza da attacchi risultano nella media (a parte il 6 considerato in genere con un impatto superiore).

Tabella 68: check-list del cluster D

Check-list strumenti per cluster D		
Comuni	2 (n.f.)	Collaborazione tra dipendenti
	3 (n.f.)	Integrità, lealtà dei dipendenti
	5 (n.f.)	Aspetti soft
	6 (n.f.)	Continuous improvement
	8	Segnalare incidenti e debolezze
	10 (n.f.)	Valutazione della conformità di sicurezza
	11	Partnership
Caratteristici	**4 (n.f.)**	**Sviluppo della consapevolezza interna sulla sicurezza**
	12 (n.f.)	**Sviluppo della consapevolezza sulla sicurezza con i miei partner**
	13 (n.f.)	**Riduzione della differenza di cultura tra aziende e partner**
Non utilizzati	1	Forza multidisciplinare
	7	Business continuity planning
	9	Knowledge management
	14	Focus sul cliente

Il quarto cluster è caratterizzato da:

- Dimensione piccola
- Integrazione bassa
- Ambito stradale

Come evidenziato per il cluster B, diminuendo la dimensione vi è una differenza nella modalità di applicazione degli strumenti (da formale a non formale) per i motivi spiegati in precedenza. In questo cluster si possono individuare casi eccellenti di applicazione degli strumenti 2, 3 e 8. Il motivo è che questi tre strumenti sono molto importanti in un contesto con alta variabilità degli imprevisti così da poter reagire prontamente a qualsiasi situazione facendo della flessibilità il proprio fattore critico di successo. A conferma di ciò si può notare dagli specifici grafici utilizzo/importanza come gli strumenti (soprattutto 2 e 8) siano molto utilizzati e considerati molto importanti. È interessante notare come l'impatto di questi strumenti sulla sicurezza di fornitura sia però molto basso, mentre su quella di attacchi solo lo strumento 8 concorra in modo deciso al miglioramento di quest'ultima (riferimento: Tabella 49, Tabella 51, Tabella 53, Tabella 55, Tabella 56 e Tabella 59).

Tabella 69: check-list del cluster E

Check-list strumenti per cluster E		
Comuni	2	Collaborazione tra dipendenti
	3	Integrità, lealtà dei dipendenti
	5	Aspetti soft
	6	Continuous improvement
	8 (n.f)	Segnalare incidenti e debolezze
	10	Valutazione della conformità di sicurezza
	11	Partnership
Caratteristici	**1**	**Forza multidisciplinare**
	4 (n.f.)	**Sviluppo della consapevolezza interna sulla sicurezza**
	7	**Business continuity planning**
	9 (n.f.)	**Knowledge management**
Non utilizzati	12	Sviluppo della consapevolezza sulla sicurezza con i miei partner
	13	Riduzione della differenza di cultura tra aziende e partner
	14	Focus sul cliente

Il quinto cluster è caratterizzato da:

- Dimensione grande
- Integrazione alta
- Ambito ferroviario

Questa tipologia di azienda è quella che meglio riesce ad applicare lo strumento 7 data la sua forza contrattuale e la sua vicinanza al trazionista, come testimoniato dalla Tabella 73. Questo strumento però dimostra avere poco impatto sulle prestazioni di sicurezza di attacchi e fornitura. Gli strumenti non utilizzati da questa tipologia di aziende sono esterni, legati alla crescita dei partner e alla riduzione delle differenze e allo sviluppo dei un'ottica di filiera. Il motivo risiede nel fatto che il cliente industriale non viene mai a contatto con chi si occupa solo di ferrovia; la mancanza di questa interfaccia non stimola queste aziende a sviluppare questi strumenti (nessuna azienda che si interfaccia con la ferrovia ha menzionato gli strumenti 12, 13 o 14 come importanti).

Tabella 70: check-list del cluster E

Check-list strumenti per cluster F		
Comuni	2 (n.f.)	Collaborazione tra dipendenti
	3 (n.f.)	Integrità, lealtà dei dipendenti
	5 (n.f.)	Aspetti soft
	6 (n.f.)	Continuous improvement
	8 (n.f.)	Segnalare incidenti e debolezze
	10 (n.f.)	Valutazione della conformità di sicurezza
	11	Partnership
Caratteristici	**1 (n.f)**	**Forza multidisciplinare**
Non utilizzati	4	Sviluppo della consapevolezza interna sulla sicurezza
	7	Business continuity planning
	9	Knowledge management
	12	Sviluppo della consapevolezza sulla sicurezza con i miei partner
	13	Riduzione della differenza di cultura tra aziende e partner
	14	Focus sul cliente

Il sesto cluster è caratterizzato da:

- Dimensione piccola
- Integrazione alta
- Ambito ferroviario

Lo strumento 1, che rappresenta una costante per chi si interfaccia lato ferrovia, è presente anche in questa tipologia di azienda ma informalmente date le dimensioni. Lo strumento 7 invece è possibile applicarlo solo se viene effettuata la trazione internamente (quindi se vi è un'alta integrazione lato ferrovia), mentre risulta impraticabile se l'integrazione è raggiunta lato strada. La percezione delle aziende di questo cluster in termini di importanza è rivolta soprattutto verso gli strumenti 2 e 8 anche se non giustificato dagli impatti che questi ultimi hanno sulla sicurezza di fornitura; la giustificazione deriva dall'elevato impatto sulla sicurezza da attacchi, soprattutto per quanto riguarda lo strumento 8.

Tabella 71: check-list del cluster G

Check-list strumenti per cluster G		
Comuni	2	Collaborazione tra dipendenti
	3	Integrità, lealtà dei dipendenti
	5	Aspetti soft
	6	Continuous improvement
	8 (n.f.)	Segnalare incidenti e debolezze
	10	Valutazione della conformità di sicurezza
	11	Partnership
Caratteristici	**1**	**Forza multidisciplinare**
	4 (n.f.)	**Sviluppo della consapevolezza interna sulla sicurezza**
	9 (n.f.)	**Knowledge management**
Non utilizzati	7	Business continuity planning
	12	Sviluppo della consapevolezza sulla sicurezza con i miei partner
	13	Riduzione della differenza di cultura tra aziende e partner
	14	Focus sul cliente

Il settimo cluster è caratterizzato da:

- Dimensione grande
- Integrazione bassa
- Ambito ferroviario

Data la grossa dimensione, viene applicato lo strumento 4. Questo però risulta più importante per l'ambito stradale (applicazione formale per i cluster A e C), mentre in questo contesto viene applicato informalmente. Vengono esclusi gli strumenti esterni 12, 13 e 14 per i motivi esposti nel cluster E. Lo strumento 7 risulta di impossibile applicazione date le esigue possibilità di influenzare il trazionista.

Si evidenzia il fatto che, per quanto riguarda i fattori di contesto caratteristici del cluster, lo strumento 9 risulta avere molti impatti sulla sicurezza di fornitura ma impatti medio-bassi per la sicurezza da attacchi.

Tabella 72: check-list del cluster H

Check-list strumenti per cluster H		
Comuni	2 (n.f.)	Collaborazione tra dipendenti
	3 (n.f.)	Integrità, lealtà dei dipendenti
	5 (n.f.)	Aspetti soft
	6 (n.f.)	Continuous improvement
	8 (n.f.)	Segnalare incidenti e debolezze
	10 (n.f.)	Valutazione della conformità di sicurezza
	11	Partnership
Caratteristici	**1 (n.f.)**	**Forza multidisciplinare**
Non utilizzati	4	Sviluppo della consapevolezza interna sulla sicurezza
	7	Business continuity planning
	9	Knowledge management
	12	Sviluppo della consapevolezza sulla sicurezza con i miei partner
	13	Riduzione della differenza di cultura tra aziende e partner
	14	Focus sul cliente

L'ultimo cluster è caratterizzato da:

- Dimensione piccola
- Integrazione bassa
- Ambito ferroviario

In questa categoria troviamo come strumento caratteristico solo la forza multidisciplinare. Le aziende che fanno parte di questo cluster si occupano in genere solo del trasbordo delle ILU, sono cioè dei piccoli gestori di terminal intermodali in cui è presente un'elevata varietà di attività da svolgere come descritto nel paragrafo 6.2.3. Lo strumento è applicato in modo informale date le esigue dimensioni aziendali e l'impatto principale è sulla sicurezza da attacchi. Tutti quegli strumenti orientati alle prestazioni di filiera (12, 13 e 14) sono invece non applicati visto il ristretto ambito di attività e responsabilità. Gli strumenti 4 e 3 non sono di vitale importanza come per altre aziende in quanto, avendo un rapporto personale con ogni dipendente date le esigue dimensioni, è più facile ed immediata la diffusione di una consapevolezza sulle tematiche di sicurezza (4) e di codici di comportamento (3).

6.4 Best practice

Di seguito si riporta la Tabella 73 in cui vengono sintetizzate le principali best practice riscontrate durante le interviste sul campo.

Tabella 73: Best practices

Azienda	Strumento	Descrizione
Hoyer	(1) Forza lavoro multidiscplinare	L'azienda di base applica un programma di formazione rivolto agli autisti che consente loro di poter gestire qualsiasi tipologia di merce trasportata dall'azienda sia per quanto riguarda le modalità di trasporto che per quelle di carico/scarico. In aggiunta gli viene fatta una formazione specifica relativa ai prodotti trasportati, così da renderli agli occhi dei clienti dei veri e propri

		esperti del prodotto. Gli autisti hanno così anche il compito di spiegare ai clienti tutti i rischi associati ai prodotti, dare consigli sulle corrette modalità di gestione, oltre a poter fare controlli di conformità e verifiche delle attrezzature dei clienti.
BAS	(2) Collaborazione tra dipendenti	Bas implementa la politica del mentore. Per ogni categoria di autisti viene associato un autista mentore, solitamente il più esperto. Il mentore è il punto di riferimento in caso di qualsiasi tipologia di problema e diventa di fatto il responsabile del gruppo. Il mentore diventa il punto di congiungimento tra la pianificazione e il lato operativo e partecipa a tutte le riunioni periodiche organizzate dall'azienda con i manager e i responsabili della pianificazione. Vengono inoltre coinvolti nelle riunioni annuali con le filiali estere dell'azienda, nelle quali tutti i mentori del gruppo BAS si ritrovano.
MDB	(2) Collaborazione tra dipendenti	MDB utilizza un sistema strutturato di incentivazione MbO (Management by Objective). Il sistema prevede di assegnare degli obiettivi individuali e di squadra a tutti i dipendenti d'azienda (tra cui anche obiettivi di "sicurezza") e di riconoscere un incentivo economico sulla base degli obiettivi raggiunti.
Sogemar	(2) Collaborazione tra dipendenti	Gestione di tutti i dipendenti in team (a cui viene assegnato il colore rosso, blu, giallo etc.). I team sono messi in competizione tra loro e a fine anno viene assegnato un incentivo economico per il team che si è dimostrato più meritevole. Una figura in azienda ha la responsabilità di formare, gestire ed eventualmente modificare i team, per renderli più performanti possibile.
BAS	(3) Integrità e lealtà dei dipendenti	L'azienda ha una politica strutturata che segue tutto il percorso di crescita di un dipendente in azienda. Ci sono dei passaggi e rituali predefiniti come per esempio una cerimonia nella quale il proprietario conferisce una spilla d'ora con il simbolo aziendale agli autisti con dieci anni di servizio in azienda.
Hoyer	(4) Sviluppo della consapevolezza interna sulla sicurezza	Ogni volta che si verifica un incidente di security sono tempestivamente convocate le "security flash", ovvero riunioni d'urgenza di breve durata nelle quali tutti gli autisti vengono invitati per essere aggiornati sulla tipologia e sulla natura dell'incidente, sui rischi, sulle nuove procedure e sulle precauzioni da prendere.
Hupac	(6) Continuous improvement	A Periodi fissi sono presenti delle opportinità per tutti i dipendenti per avere un colloquio individuale con il Direttore Generale d'azienda. Inoltre in azienda è presenta una cassetta delle idee per chi volesse fare delle segnalazione o dare dei suggerimenti rimanendo

		anonimo.
Hoyer	(6) Continuous improvement	Costituzione di team per l'investigazione su incidenti o vulnerabilità specifiche d'azienda. Nel team sono compresi, oltre ai capiarea e ai responsabili della pianificazione, anche un autista (sempre a stretto contatto con il job), e il driver training (responsabile degli autisti) per dare suggerimenti pratici per l'implementazione di misure correttive. Dal team si creano le nuove working instruction che verranno diffuse a tutti gli altri operatori
Hupac	(7) Business continuity planning	Unità di crisi per la gestione degli assi ferroviari in situazioni di emergenza e definizione di tracce alternative per i collegamenti ferroviari maggiormente sfruttati dall'azienda.
Interporto di Rivalta	(7) Business continuity planning	Per i maggiori clienti vengono concordate a priori delle modalità di trasporto di backup in caso di impossibilità di effettuare il trasporto intermodale.
Fercam	(9) Knowledge management (in via di progettazione)	Si sta sviluppando un software di CRM per la codifica delle esperienze, con un database integrato e disponibile per tutte le filiali del gruppo. Il software oltre a raccogliere le informazioni su tutti gli incidenti occorsi (con specificazione sulla natura, sulle cause etc.) ha una sezione apposita per raccogliere e condividere la informazioni relative ai rischi e alle procedure di sicurezza.
Hoyer	(9) Knowledge management	Piattaforma intra-aziendale con un database condiviso. La piattaforma presenta una sezione che riporta le prestazioni mensili di sicurezza e le presentazioni relative alla security che sono accessibili a tutti i dipendenti. Un'altra sezione racchiude tutte i programmi di formazione per gli autisti, un'altra riporta tutte gli incidenti che si sono verificati e un'altra tutti i rischi associati ad un determinato prodotto e tutte le situazioni di near misses.
Marenzana	(8) Segnalare incidenti e debolezze	Gli autisti ogni volta che si verifica un incidente (o un near misses) devono compilare una chek-list predefinita, che poi viene utilizzata per alimentare il database aziendale sugli incidenti avvenuti (o potenziali).
Fercam	(8) Segnalare incidenti e debolezze	L'azienda ha creato delle figure professionali che hanno lo scopo di occuparsi della gestione di incidenti o rischi suddivisi per tipologia di merce trasportata, modalità di trasporto (tratto stradale o ferroviario) e tipologia di ILU.

Hoyer	(8) Segnalare incidenti e debolezze	Per ogni main incident (e in alcuni casi particolari anche per i near misses) parte un sistema di incident investigation che prevede la compilazione di un form nel quale devono essere esplicitate la tipologia di incidente, le cause che l'hanno provocato e le eventuali azioni preventive o correttive.
Fercam	(14) Focus sul cliente	Instaurazione con i clienti finali maggiormente sensibili alle tematiche di sicurezza di un sistema di KPI che riguarda la filiera intermodale nel complesso. L'incentivazione associata ad una buona prestazione di filiera non è di tipo economico ma legato all'aumento dei volumi dei trasporto.

6.5 Criticità, tendenze e opportunità dell'intermodale

Dall'analisi empirica, abbiamo riscontrato dei temi che trasversalmente interessano le aziende intervistate rispetto alla gestione del servizio intermodale e al suo sviluppo futuro, riportati di seguito:

Il ruolo delle informazioni

Confrontando quanto emerso dalla letteratura con i reali comportamenti delle aziende è emersa una discrepanza in riferimento alla trasparenza e alla visibilità all'interno della SC (paragrafo 2.3.4). Infatti in letteratura, solo Nassimbeni (2009) mette in luce il trade-off tra condivisone di informazioni e segretezza, mentre generalmente la diffusione e la condivisione di informazioni è considerata un rinforzo positivo alla sicurezza della SC e, di riflesso, di tutte le aziende che ne fanno parte. Nella realtà, invece, per molte aziende esiste un serio trade-off nella scelta di diffondere informazioni a tutti i livelli dell'organizzazione; infatti se è verificato che per la sicurezza di fornitura la condivisione di informazione nella SC ha impatti esclusivamente positivi, per quella da attacchi non è sempre vero. Molte aziende ritengono infatti che la condivisione di informazioni estesa al livello operativo sia legata (di fatto o potenzialmente) all'aumento degli episodi collusivi, soprattutto per quanto riguarda possibili accordi tra differenti attori della SC (per esempio accordi tra chi lavora in un terminal e gli autisti dei vettori stradali). Il tema è sentito più che altro dagli operatori terminalistici, che ogni giorno devono gestire un numero rilevante di ILU. Da un lato la condivisione di informazioni è ritenuta indispensabile per migliorare la collaborazione orizzontale e verticale ma dall'altro è considerata una fonte di rischio. Le risposte pratiche delle aziende a questo trade-off sono differenti anche se, generalizzando, è possibile

individuare due tipologie di risposte alternative: alcune aziende preferiscono risolverlo non divulgando le informazioni inerenti il contenuto delle ILU agli operatori (limitando queste informazioni alla sola pianificazione), mentre altre hanno deciso di investire sui sistemi di controllo del lavoro, per limitare la possibilità che i propri dipendenti siano coinvolti in episodi collusivi. Il tema può essere esteso anche alla SC, dove però il focus passa dalla scelta se divulgare o meno le informazioni, alla sicurezza dei metodi di comunicazione tra le azienda. Se infatti a livello di filiera è indispensabile che le informazioni circolino, i mezzi di comunicazione devono garantire la riservatezza e la sicurezza della trasmissione alle sole aziende. In questo senso tutti gli strumenti e le tecnologie relativi all'Information management (paragrafo 3.2.5) sono una risposta al problema.

Il vantaggio dell'integrazione verticale

Abbiamo già descritto come una filiera come quella intermodale abbia necessità di lavorare in modo integrato e con un'ottica comune per ottenere performance di alta sicurezza e, più in generale, di alta qualità (quello che abbiamo definito come avere un'ottica sul cliente finale, paragrafo 4.3.2). In risposta a questa necessità la tendenza attuale delle grandi aziende è quella di integrarsi verticalmente lungo la filiera, spesso con la costituzione di un company train. Già Debernardi (1997) aveva considerato come gli operatori intermodali avessero la necessità di integrarsi verticalmente nella filiera per rispondere alle complessità gestionali del settore. Con la liberalizzazione del mercato ferroviario, si sta infatti sviluppando una modalità di gestione integrata del trasporto end-to-end, anche se attualmente la modalità di gestione più diffusa è tramite shuttle train organizzati da operatori ferroviari esterni. Questa tendenza è confermata anche dalle aziende presenti nel nostro campione, come Fercam, Ewals e Sogemar. Fercam si sta infatti attrezzando per costituire un company train, acquistando i carri, la locomotrice e il personale per effettuare la trazione da una società ferroviaria per aumentare la propria integrazione verticale. Ewals allo stato attuale organizza invece shuttle train composti esclusivamente da ILU dell'azienda, però non possiede ancora i carri ferroviari e i locomotori. Sogemar ha invece da poco fondato una società di trazione ferroviaria e nel prossimo futuro potrà gestire in prima persona l'intero trasporto. L'obiettivo generale, oltre all'aumento della visibilità, sembra essere quello di slegarsi dalle performance del trazionista ferroviario e sfruttare la possibilità di ottimizzare al meglio il trasporto. Come detto da Gianfranco Brillante *"oggigiorno*

utilizziamo dei vettori ferroviari come consolidatori, per i quali noi siamo uno tra i tanti clienti. […] oltre a questi ci stiamo attrezzando per costituire un company train, ovvero abbiamo comprato un treno da una società di trazione ferroviaria, che opera solo con noi. Abbiamo a disposizione i vagoni, i locomotori e il personale per fare la trazione e noi caricheremo tutte le nostre casse su quel treno. Facendo questa operazione pensiamo di ottenere un miglioramento notevole della qualità perché possiamo controllare il treno. Potremmo sapere con esattezza a che ora parte e a che ora arriva, riusciremo a determinare le tracce in modo preciso perché essendoci solo le nostre casse effettueremo sempre la stessa tratta. Il rischio è ovviamente quello di non poter garantire un numero adeguato di casse per riempire il treno, che però si può riuscire a calcolare mediamente". La gestione di un company train presenta molti vantaggi ma porta anche diverse criticità. In una situazione di economia fluttuante un investimento in capitale fisso (come quello necessario in questa situazione) di grosse dimensione potrebbe comportare una notevole perdita di flessibilità per l'azienda, che può portare a sostanziali perdite economiche nei periodi di recessione della domanda. Una soluzione possibile (quella che adotterà Fercam appunto) è quella di gestire company train sulle tratte più importanti, con volumi di traffico stabili e massa critica significativa (e possibilmente anche ben equilibrate in termini di differenza di saturazione tra andata e ritorno), e affidarsi ad operatori ferroviari, utilizzati come consolidatori, per gestire le restanti ILU.

La focalizzazione del servizio intermodale

Legato al tema dell'integrazione verticale vi è quello della focalizzazione, intesa in due differenti termini: da un lato la focalizzazione a livello operativo del servizio intermodale su specifiche tratte geografiche e dall'altra la focalizzazione dell'azienda nel suo complesso nell'offerta di business, intesa come differenziazione dell'offerta intermodale. In riferimento alla differenziazione dell'offerta, Ewals per esempio a partire dal 2008 ha creato la Business Unit "Ewals Intermodal" che gestisce a 360 gradi l'offerta di servizi intermodali della capogruppo Ewals Cargo Care, con l'obiettivo di sfruttare al meglio la richiesta di trasporto intermodale. La netta differenziazione del servizio combinato strada-ferrovia rispetto a quello monomodale aiuta infatti nell'evidenziare le qualità distintive di questa modalità di trasporto che troppo spesso viene confrontata con le altre modalità esclusivamente dal punto di vista economico, tralasciandone le caratteristiche distintive (sicurezza da attacchi ed eco-compatibilità

principalmente). Con riferimento invece alla focalizzazione a livello operativo su un numero ristretto di tratte, è possibile ottenere un miglioramento del controllo da parte dell'azienda sul trasporto creando le condizioni per lo sviluppo di alcuni degli strumenti culturali proposti (come il BCP, il continuous improvement, segnalazioni di incidenti e debolezze). In questo senso, per esempio, Fercam ha deciso di passare da un'offerta intermodale dispersiva, ad una focalizzata sulla direttrice Nord Italia-Benelux.

La spinta verso la qualità[62] del servizio

Un altro tema trasversale, che ostacola la necessità del trasporto intermodale di imporsi come una modalità di trasporto altamente sicura, è la mancanza di politiche che incentivino le performance di alto livello qualitativo**.** Questa è una mancanza importante, perché l'intermodale per poter essere realmente competitivo (soprattutto su tratte di corto o medio raggio) deve puntare sulla maggiore qualità del servizio rispetto ad altri sistemi di trasporto. Le radici del problema stanno nello scarso potere contrattuale che gli MTO hanno nei confronti del cliente finale, con ripercussioni su tutti gli attori della filiera; tutti gli MTO intervistati, infatti, hanno evidenziato come non esistano nei contratti in essere degli incentivi legati alle performance di tipo economico, e sono molto rari anche gli incentivi di natura non economica (come un aumento dei volumi). Non essendo incentivato il MTO, non si impegna nel trasmettere agli attori più "interni" un'attenzione al miglioramento delle performance di qualità. Essendo il trasporto intermodale una modalità più sicura (dal punto di vista degli attacchi) e più sostenibile di quella monomodale, sarebbe opportuno incentivare le ottime performance anche dal punto di vista della puntualità di consegna, così da poter allineare tutta la filiera alle esigenze del cliente finale. Con questa politica sarebbe anche possibile discriminare chi lavora con standard qualitativamente alti, con vantaggi di "reputazione" del trasporto intermodale. Nella realtà, gli unici casi isolati di comportamenti eccellenti sono da ricercare nell'azione di grosse multinazionali della GDO, che sotto la spinta della recente sensibilizzazione verso le tematiche di compatibilità ambientale, hanno scelto di aumentare la quota di trasporto intermodale rispetto a quello "tutto strada". Si tratta però ancora di casi isolati, anche se la continua crescita delle peformance green delle aziende potrebbe essere un fattore determinante per lo sviluppo dell'intermodale.

[62] Nel termine qualità sono compresi i concetti di sicurezza (attacchi e fornitura), efficacia ed eco-compatibilità.

La percezione della ferrovia da parte delle industrie dell'opinione pubblica

Un grosso limite allo sviluppo della ferrovia in Italia è la percezione consolidata negli anni che il trasporto ferroviario sia inefficiente e inefficace dal punto di vista infrastrutturale e gestionale. Questa convinzione è stata supportata negli anni da una mancanza di coerenza politica negli strumenti di incentivazione e dalla tradizione culturale italiana (paragrafo 1.5). Emblematica è la situazione del gruppo Ferrovia dello Stato che non nasconde la sua volontà di voler osteggiare il trasporto ferroviario di merci, per favorire quello delle persone; in realtà gli scarsi investimenti sull'infrastruttura di rete, sommati a lacune di tipo gestionale, hanno portato sia le industrie che l'opinione pubblica a considerare il trasporto ferroviario inefficiente e di bassa qualità. In realtà con una politica di investimento in tecnologie e infrastrutture lo sviluppo del traffico merci non pregiudicherebbe quello del traffico persone. L'esempio della Germania è eclatante in questo senso: lo sviluppo infrastrutturale ha consentito, dove possibile, di sdoppiare la rete merci da quella persone e l'utilizzo di nuove tecnologie ha consentito, dove questo non è stato possibile, di migliorare l'integrazione delle due modalità di trasporto (vedi scambi binari automatici e gestione dei flussi real time che permettono la gestione integrata delle tracce dei treni per merci e persone). Inoltre la spinta verso l'ottimizzazione delle pratiche gestionali legate alla gestione dei treni, iniziate per scopi industriali, si sono diffusi fino al settore del traffico persone, con benifici reciproci (condividendo la stessa infrastruttura). Da parte dell'opinione pubblica, in Italia, oltre a ritenere il trasporto ferroviario inefficiente, è anche diffuso il sentimento che il trasporto ferroviario sia poco sicuro; questo a causa della maggior portata e degli effetti mediatici derivanti che gli incidenti ferroviari hanno rispetto a quelli stradali (vedi il recente incidente a Viareggio nel 2009). In realtà nel trasporto merci su rotaia il rischio di incidenti è 40 volte inferiore rispetto a quello su strada[63]; sia l'opinione pubblica che i clienti industriali non sono ancora sufficientemente informati e sensibili su questo tema.

6.6 Conclusioni

In questo capitolo abbiamo effettuato tutte le analisi necessarie per poter rispondere alle domande di ricerca. In relazione alla prima e alla seconda abbiamo eseguito l'analisi sul totale del campione di aziende intervistate così da comprendere quali siano gli

[63] www.hupac.ch

strumenti, tra quelli proposti, più utilizzati e quali siano i loro impatti sulle prestazioni di sicurezza. È seguita l'elaborazione dei dati in base ai fattori di contesto tramite l'aggregazione di questi in base alle caratteristiche dimensionali, di integrazione verticale e di appartenenza ad uno specifico ambito. Questo ci ha consentito di osservare se i fattori di contesto sono delle discriminanti per:

- l'applicazione degli strumenti (domanda di ricerca n°3);
- l'impatto degli strumenti sulle prestazioni finali di sicurezza (domanda di ricerca n°4);
- l'impatto dei fattori causa sulle prestazioni di sicurezza (domanda di ricerca n°5).

Abbiamo redatto delle check-list di strumenti adottati dalle aziende in funzione degli specifici fattori di contesto, per proporre gli strumenti da applicare per raggiungere delle prestazioni in linea con il settore. In ultimo, con l'ausilio di mappe causali, abbiamo evidenziato delle particolarità legate all'utilizzo e agli impatti di strumenti e fattori causa evidenziando le aree di miglioramento. Abbiamo infine concluso effettuando alcune considerazioni su tematiche trasversali del trasporto intermodale emerse a margine delle interviste.

Rileviamo infine i limiti dell'analisi effettuata. Il primo riguarda il campione di aziende analizzato che, pur essendo eterogeneo, non può fornire la base per un'analisi di tipo quantitativo/statistico data l'esigua dimensione. Per questo motivo nello sviluppo del modello abbiamo cercato di compiere un'astrazione (considerando i fattori di contesto) senza effettuare delle analisi puntuali sulle aziende, che avrebbero portato a risultati troppo legati alle caratteristiche specifiche delle stesse. Un'altra approssimazione riguarda il calcolo della percentuale di impatto dei fattori causa sulle prestazioni di sicurezza spiegate nel paragrafo 5.3. Ai fini di svolgere un'analisi più robusta dal punto di vista quantitativo sarebbe necessario avere accesso ai database aziendali, per ricavare l'esatta percentuale storica di incidenza dei fattori causa rispetto ai KPI di sicurezza limitando così le approssimazioni. Sommando queste condizioni, si potrebbe creare un modello che consenta un'analisi più robusta dal punto di vista quantitativo. Evidentemente, passando dalle informazioni soggettive dei manager intervistati a quelle basate su dati storici, si migliorerebbe la robustezza quantitativa del modello, anche se dall'altro si perderebbe la visione d'insieme che il manager, data l'esperienza nel settore, può fornire. In particolare quest'ultima è molto importante data la natura dello studio; per quanto riguarda infatti l'attribuzione di un motivo (fattore causa) della

cattiva prestazione di sicurezza (furti, ritardi) riteniamo che a volte la sensazione del manager si avvicini maggiormente alla realtà rispetto ai casi documentati in un database. Un esempio può essere legato al fattore causa collusione: a seguito di un furto non è semplice dimostrare se la causa sia da attribuire ad una lacuna procedurale piuttosto che ad un episodio collusivo. Concludendo, l'ideale sarebbe dunque allargare la base del campione di aziende analizzate includendo nel modello sia informazioni di natura quantitativa che di natura qualitativa, evidenziandone tendenze e trade-off.

7 Conclusioni

7.1 Ambito di ricerca[64]

Il nostro lavoro di Tesi si focalizza sulla sicurezza all'interno delle ILU supply chain. Con il termine ILU supply chain, intendiamo l'insieme di organizzazioni e attori che interagiscono tra di loro per portare dall'origine a destino il flusso di ILU (Intermodal Load Unit), ossia container, casse mobili e semirimorchi (IMCOSEC, 2010).

All'interno delle ILU supply chain il nostro focus è rivolto al trasporto intermodale strada-ferrovia, in particolare quello combinato che prevede la parte più consistente del trasporto effettuata su rotaia, mentre il primo e l'ultimo miglio effettuati su strada. I benefici caratteristici di questo nuovo approccio al trasporto sono da ricercare in prestazioni sociali (riduzione del traffico su strada), di sicurezza (utilizzato soprattutto per prodotti chimici pericolosi), energetiche (minor dispendio di energia) e di sostenibilità ambientale (riduzione di inquinanti atmosferici). Riconoscendo questi vantaggi, che esulano da un'analisi prettamente economica, l'Unione Europea ha effettuato svariati studi e intrapreso una serie di programmi in favore del trasporto intermodale. L'obiettivo di questi programmi è il bilanciamento nell'utilizzo delle diverse modalità di trasporto (strada, ferrovia, mare, vie navigabili interne, aereo); ad oggi il sistema di trasporto europeo è fortemente sbilanciato verso il trasporto su strada e in generale verso l'utilizzo di mezzi non sostenibili dal punto di vista ambientale ed energetico. Passando alla situazione italiana, allo stato attuale, le maggiori criticità che ostacolano lo sviluppo del trasporto intermodale sono di:

- natura infrastrutturale, inerenti sia l'assenza di interconnessioni fra le reti sia le differenze nella sagoma limite all'interno della rete ferroviaria;
- natura gestionale, legata alle caratteristiche intrinseche del trasporto intermodale. Coesistono infatti numerosi attori che svolgono operazioni diverse e non sempre hanno piena visibilità l'uno sull'altro; oltretutto il trasporto intermodale è meno flessibile di quello stradale e complica l'attività di ricerca di carichi per la tratta di ritorno;

[64] Scritto in collaborazione con l'Ing. Fulvio Quattroccolo, fondatore e gestore del sito web www.intermodale24-rail.net

- natura giuridica, riguardante in modo particolare il differente stato di attuazione delle direttive europee come quella sulla liberalizzazione del mercato ferroviario della trazione: gli ex-monopolisti (in Italia Trenitalia Cargo) sono i soli ad avere i certificati di sicurezza su tutta la rete, quindi di fatto su alcune tratte hanno ancora il monopolio; questo impedisce lo sviluppo di una reale concorrenza con effetto sull'efficienza nei trasporti e sui prezzi richiesti;
- assenza di una chiara divisione dei ruoli; in particolare si fa riferimento al ruolo dominante di alcune imprese che ricoprono contemporaneamente più ruoli e hanno partecipazioni in loro competitor, loro fornitori e loro clienti. Questa situazione potrebbe comportare interferenze sull'operatività quotidiana (favoreggiamento della partecipata) limitando di fatto lo sviluppo del trasporto intermodale.

Il trasporto intermodale strada-ferrovia può essere classificato secondo diverse dimensioni come la tipologia di ILU trasportata (container, casse mobili o semirimorchi), il sistema di trasporto (accompagnato o non accompagnato) o la tipologia di treno adottata (treno completo tra cui sistemi diretti, shuttle e gateway oppure treno a carico singolo). I ruoli atomici all'interno della filiera intermodale, individuati nel corso delle interviste, sono schematizzati in Figura 52.

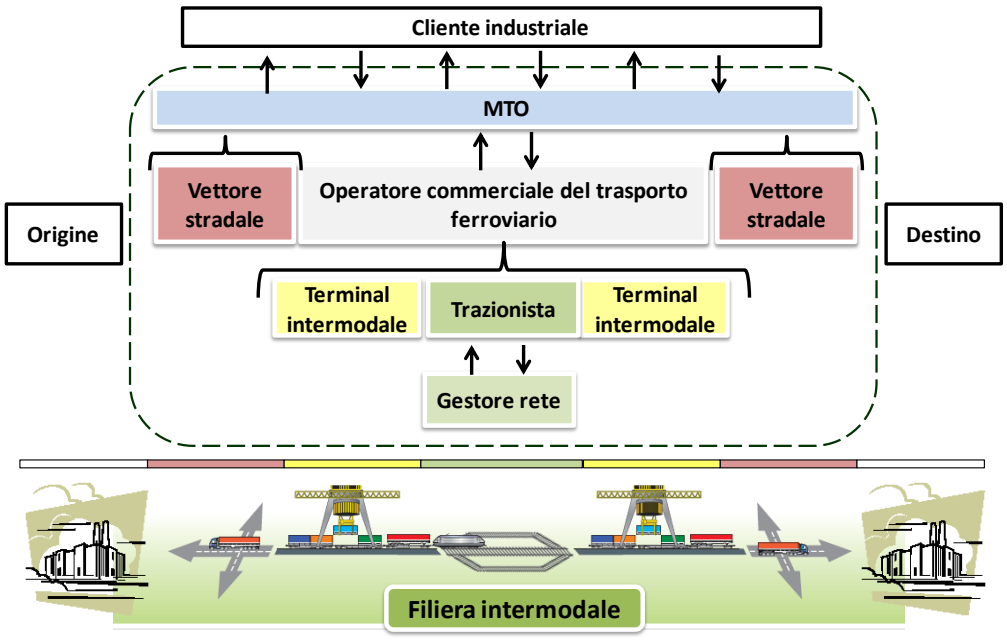


Figura 52: classificazione dei vari attori della filiera intermodale strada-ferrovia

7.2 Analisi della letteratura

Per quanto riguarda il termine sicurezza, invece, abbiamo inizialmente preso in considerazione tutte le sue possibili accezioni. Dalla letteratura risulta che non esiste un significato univoco del concetto di sicurezza in quanto il termine italiano comprende due accezioni completamente diverse che vengono meglio espresse dai termini inglesi *security* e *safety*. Il primo corrisponde alla sicurezza del patrimonio tangibile e intangibile di un sistema[65], mentre il secondo riguarda la sicurezza delle persone, intesa come loro incolumità. Oltretutto la sicurezza può essere intesa in diversi modi anche in base all'approccio con cui essa viene analizzata che può essere di tipo normativo, manageriale, pratico, sociologico, organizzativo, tecnico, ingegneristico etc. In particolare ci siamo occupati della sicurezza del sistema di trasporto intermodale, quindi intesa come security, secondo l'approccio manageriale, organizzativo, sociologico e solo marginalmente tecnico.

Anche le organizzazioni hanno appreso il concetto di sicurezza secondo sfumature diverse. Le prime ricerche si sono incentrate su tematiche sociologiche e psicologiche, focalizzandosi sull'incolumità e il benessere delle persone. La preoccupazione di mettere al sicuro i propri beni durante il trasporto è emersa invece in letteratura soprattutto negli ultimi anni, con l'introduzione del concetto di Supply Chain Security (SCS).

Con SCS si intende un approccio che prevede l'applicazione di programmi, sistemi, procedure, tecnologie e soluzioni per affrontare le minacce a cui sono soggette le supply chain con l'obiettivo di migliorarne la sicurezza (Donner e Kruk, 2009; Closs e McGarrell, 2004; Burmeisters e Solovjovs, 2009).

A partire dal 11 settembre 2001 si è diffusa maggior consapevolezza tra le aziende sulle tematiche di sicurezza ed è iniziato il processo di cambiamento dell'approccio di SCS. In Figura 53 sono riassunti i principali cambiamenti, in parte ancora in corso.

[65] www.businessdictionary.com

	Prima	→	Dopo
Misure	Prevenzione furti	→	Prevenzione furti e anti-terrorismo
Approccio	Funzionale	→	Integrato
Iniziativa	Pubblica o privata	→	Pubblica e privata
Estensione	Nazionale/locale	→	Globale
Focus	Azienda	→	End-to-end supply chain
Visibilità	1st-tier suppliers	→	2nd, 3rd-tier suppliers
Supporto	Contingency Planning	→	Contingency Planning & Crisis Mgmt
Impatto	Operativo	→	Strategico

Figura 53: Modello per il cambiamento dei requisiti della Supply Chain Security

Le organizzazioni collocano le pratiche di SCS all'interno del sistema di Risk Management. Questo denota quanto sia importante effettuare un'accurata analisi dei rischi che le supply chain corrono, attraverso cui è possibile capire le strategie di sicurezza da applicare per ridurre le vulnerabilità. In riferimento alla matrice di vulnerabilità, con cui è possibile classificare ogni fonte di rischio in funzione della probabilità di accadimento e della severità delle conseguenze, risulta che per ridurre la vulnerabilità è possibile agire su entrambe le variabili. Queste determinano la prestazione di sicurezza, che può essere dettagliata in termini di sicurezza preventiva, ossia "*la capacità di un'impresa di monitorare e prevenire possibili fattori di destabilizzazione delle sue attività"* e di resilienza, ossia "*la capacità di un'impresa che ha subito una disruption di ripristinare le normali attività"* (Nassimbeni, 2009).

In Figura 54 si osserva che le strategie di SCS variano in base ai differenti rischi della supply chain e alle condizioni di contesto.

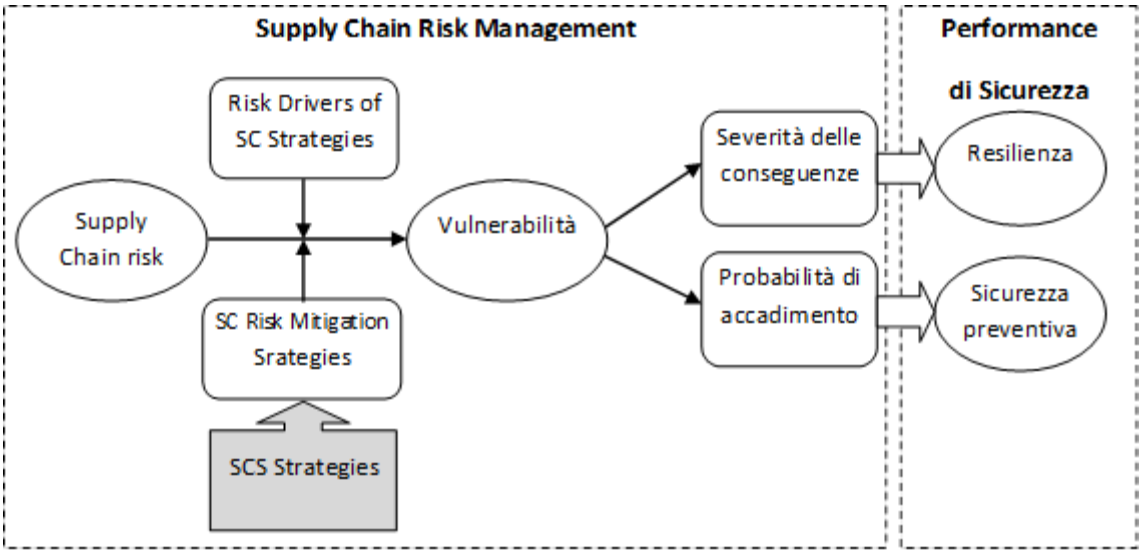


Figura 54: Supply chain risk management e performance di sicurezza

Tendenze recenti dimostrano come le organizzazioni abbiano rivolto una maggiore attenzione verso quei rischi derivanti da minacce intenzionali con conseguente focalizzazione sulle strategie che ne abbassano la probabilità di accadimento.

Dal punto di vista delle prestazioni organizzative di filiera, le strategie di SCS possono impattare anche su altre performance organizzative infatti hanno: un impatto diretto (e indiretto tramite la trasparenza) sulla sicurezza e sull'efficienza, indiretto sull'efficacia (tramite una maggiore sicurezza), e allo stesso tempo generano dei trade-off tra prestazioni di efficienza e sicurezza, come rappresentato in Figura 55. In riferimento al trade-off efficienza-sicurezza, Willis e Ortiz (2004) hanno osservato che *"se si lavora sotto le "condizioni operative normali" si potrebbero avere effetti addirittura negativi"*; Sheffi (2001) e Nassimbeni (2009) individuano nel dettaglio alcune strategie di SCS che possono portare ad un peggioramento dell'efficienza, e al contrario, strategie di supply chain efficienti che possono portare a un peggioramento della sicurezza.

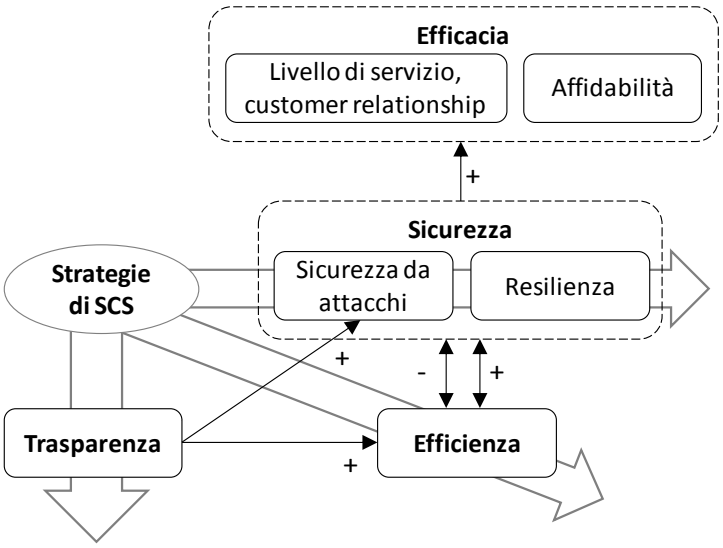


Figura 55: Mappa delle relazioni tra prestazioni organizzative

Dall'analisi delle relazioni tra SCS e prestazioni è emerso che i motivi che ostacolano la diffusione dell'approccio di SCS sono l'assenza di ricerche quantitative che dimostrino gli impatti positivi verso entrambe le prestazioni di efficienza ed efficacia, il trade-off tra le prestazioni di sicurezza ed efficienza, oltre alla mancanza di una corretta comunicazione delle pratiche di sicurezza e dei benefici ottenibili all'interno della supply chain.

L'approccio di SCS è stato successivamente declinato al nostro ambito di interesse, quello della filiera del trasporto intermodale, definita in letteratura da alcuni autori "container supply chain", o più in generale "ILU supply chain".

La globalizzazione delle aziende spiega la necessità da parte delle autorità governative e delle organizzazioni private di focalizzarsi sulla sicurezza della ILU supply chain. L'importanza di mettere al sicuro i flussi di container deriva dagli enormi rischi che corre il trasporto intermodale: infatti, più volte i container sono stati veicolo per il trasporto illegale di armi a distruzione di massa o per il trasporto clandestino di terroristi, oltre ad essere soggetti a furti e manipolazioni di ogni genere (Sarathy, 2005).

In particolare la ILU supply chain è esposta a vulnerabilità in corrispondenza di tutti gli elementi che la compongono: stabilimenti produttivi, unità di carico, fornitori, partner e organizzatori del trasporto, strutture logistiche, persone e informazioni (Sarathy, 2005, 2006).

Ulteriori difficoltà sono legate all'adozione di un approccio di SCS integrato in tutta la filiera che, insieme alla mancanza di una cultura di risk management, non permette di avere ben chiari tutti i rischi che le supply chain corrono, facendo quindi mancare il

presupposto fondamentale per la riduzione della vulnerabilità (Williams et al.,2008; IMCOSEC, 2010).

Con l'aumento dell'importanza riservata alle tematiche di SCS le autorità governative e le aziende hanno proposto dei programmi per la messa in sicurezza della catena di fornitura. Rispetto al focus tradizionale, questi nuovi programmi considerano la supply chain nella sua totalità, proponendo un approccio di collaborazione tra aziende e con le autorità governative (Donner e Kruk, 2009). In Tabella 74 sono riassunti i principali programmi ad applicazione volontaria promossi negli ultimi anni.

Tabella 74: Classificazione dei programmi volontari di sicurezza

Nome/anno di inizio	Paese di origine dell'istituto	Modalità	Partecipanti/ stato	Categoria	Obiettivo
TAPA, 1997	US	Trasporto su gomma	207 membri	Privata volontaria	Report incidenti criminali/identificazione soluzioni/condivisione informazioni
C-TPAT, 2001	US	Tutte	6375 certificazioni e 3916 aziende approvate	Governativa volontaria	Supply chain security
CSI, 2002	US	Trasporto via mare	58 porti	Governativa volontaria	Supply chain security
WCO SAFE FoS, 2005	WCO	Tutte	156 Stati membri	Internazionale volontaria	Standard per la supply chain security e per l'agevolazione del commercio
ISO 28000, 2005	Comitato tecnico ISO	Tutte	157 Paesi membri	Internazionale volontaria	Supply chain security
EU-AEO, 2008	Commissione Europea	Tutte	192 aziende	Governativa volontaria	Supply chain security e agevolazione del commercio

I nuovi approcci alla sicurezza si concentrano sulla security e hanno l'obiettivo di diffondere standard internazionali, di promuovere la diffusione e la condivisone di informazioni tra aziende e con le autorità governative, di sviluppare efficaci sistemi di gestione aziendale della sicurezza e di sviluppare dei processi che consentano una gestione integrata della filiera (Gutierrez e Hintsa, 2006). Dall'analisi dei principali programmi internazionali e della letteratura inerente alle pratiche di SCS, abbiamo ricavato la classificazione degli strumenti di sicurezza rappresentata in Figura 56.

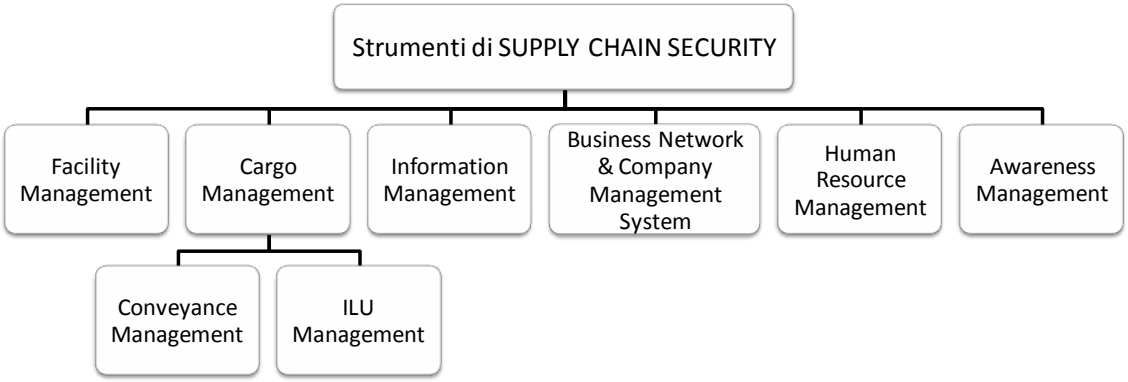


Figura 56: Classificazione ambiti SCS

La categoria "Facility Management" comprende tutti gli strumenti che consentono la messa in sicurezza delle strutture adibite all'immagazzinamento e alla gestione delle ILU; si passa da strumenti che in fase di progettazione consentono di abbassare i rischi della struttura a sistemi di difesa fisica fino a tecnologie per il monitoraggio e il controllo d'accesso. Gli strumenti di "Cargo Management" garantiscono invece la sicurezza del cargo durante tutti gli step del trasporto: in questa categoria si possono distinguere gli strumenti associati al mezzo di trasporto ("Conveyance Management") da quelli che assicurano la sicurezza della ILU rispetto a minacce intenzionali ("ILU Management"). Della prima categoria fanno parte la pianificazione delle ispezioni durante il trasporto, le soluzioni per il tracking e la gestione della rotta del cargo. Della seconda fanno parte le tecniche e le tecnologie per ispezionare le ILU e le soluzioni che vogliono impedirne la compromissione dell'integrità, di natura sia tecnologica che processuale/organizzativa. Gli strumenti di "Information Management" consentono di sfruttare le informazioni disponibili come mezzo per individuare anomalie, prevenire lacune di sicurezza e proteggere i dati critici del business. Si tratta di strumenti che permettono alle aziende di costruire un database informativo di qualità e di adottare pratiche per la salvaguardia delle informazioni e per la gestione della conoscenza in azienda. Gli strumenti della categoria "Business Network & Company Management System" consentono di rendere sicuro il sistema di gestione aziendale. Si tratta di strumenti che consentono la progettazione e l'implementazione di un sistema corporate di gestione della sicurezza e di progettare un sistema logistico flessibile e resiliente. In ottica di filiera, gli strumenti consentono la valutazione dei SC partner e l'instaurazione di relazioni collaborative con aziende ed enti governativi. Della categoria "Human Resource Management" fanno parte gli strumenti che si occupano di assicurare l'affidabilità delle persone che entrano in contatto con la ILU agendo sui processi di

selezione e di fine rapporto, sull'organizzazione dei ruoli e delle responsabilità di sicurezza in azienda. Nella categoria "Awarness Management" rientrano infine gli strumenti che garantiscono la consapevolezza sulla sicurezza del personale che entra in contatto con la ILU. Si tratta di iniziative per la formazione ed educazione del personale e per lo sviluppo della consapevolezza sulle tematiche di sicurezza in azienda e verso partner di filiera.

7.3 Disegno di ricerca

L'analisi della letteratura sulla SCS ci ha consentito di individuare nelle categorie di Information Management, Human Resource Management e Awareness Management gli strumenti meno approfonditi e sviluppati. Tali categorie hanno in comune la caratteristica di non essere strettamente legate a precisi processi o punti all'interno della supply chain, bensì sono legate al fattore umano. Abbiamo definito questi strumenti "culturali" perché agiscono su valori, motivazioni, atteggiamenti e comportamenti degli individui all'interno dell'organizzazione. Considerato lo scarso approfondimento di questi strumenti in letteratura, la loro trasversalità e l'importanza del fattore umano in relazione alla sicurezza (Lacey, 2010), abbiamo così deciso di focalizzare la nostra ricerca su di essi. Per definire al meglio il nostro disegno di ricerca abbiamo ritenuto opportuno definire il concetto di cultura organizzativa e capire la sua applicazione nelle organizzazioni in relazione alle tematiche di sicurezza. Alcuni autori hanno messo in luce la recente diffusione tra le organizzazioni del concetto di Supply Chain Security Culture (Benson, 2005; Williams et al., 2008); e di Supply Chain Security Orientation (Autry e Bobbitt, 2008; Williams et al., 2008). La loro diffusione deriva dalla combinazione di vari fattori quali il crescente focus verso le tematiche di SCS da parte delle autorità governative e le organizzazioni private, l'importanza del ruolo che le tematiche culturali ricoprono nell'influenza di obiettivi strategici, tattici e operativi delle aziende e la maggior consapevolezza che le persone di un'organizzazione e le organizzazioni stesse sono i principali responsabili della generazione di disruption, ma anche il mezzo per evitarle e porre loro rimedio (Lacey, 2010).

Sulla base di queste considerazioni, abbiamo deciso di studiare il ruolo degli strumenti di tipo culturale nello sviluppo della sicurezza delle ILU supply chain; abbiamo quindi delineato il nostro perimetro di indagine attraverso la definizione di 5 domande di ricerca:

6. Quali strumenti culturali sono adottati nelle aziende del settore intermodale?
7. Qual è l'impatto che l'applicazione di ogni strumento ha sulla prestazione di sicurezza?
8. Quali fattori di contesto spiegano l'adozione degli strumenti culturali?
9. I fattori di contesto spiegano anche gli impatti degli strumenti sulle prestazioni?
10. Quali sono i fattori causa più importanti nel determinare una cattiva prestazione di sicurezza? Sono diversi in funzione dei fattori di contesto?

Se in risposta alla domanda n° 1 sarebbe bastato effettuare delle interviste sul campo e riportarne i risultati, per rispondere alle altre domande è stato necessario costruire il modello teorico rappresentato in Figura 57, composto da quattro componenti correlate tra di loro.

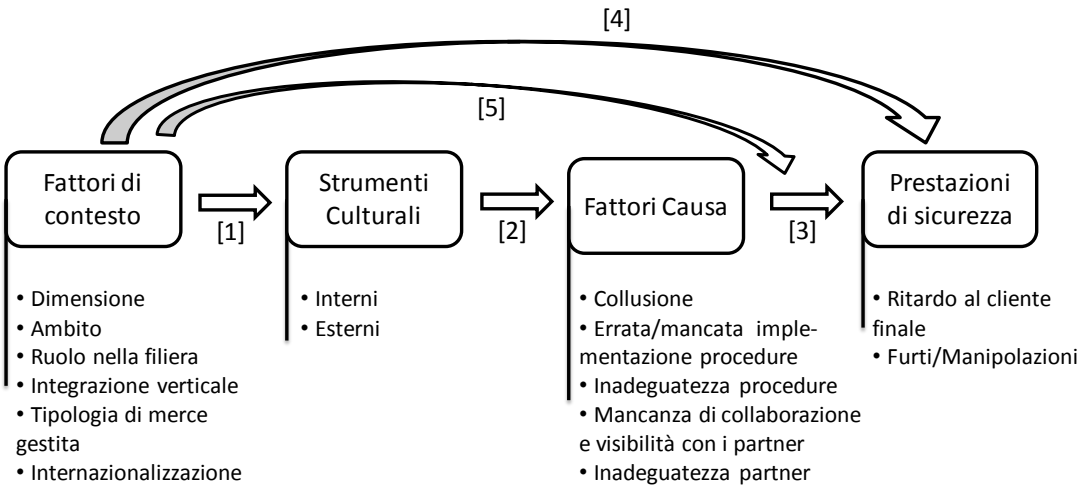


Figura 57: Modello teorico

La relazione [1] in Figura 57 presuppone l'esistenza di alcuni fattori di contesto discriminanti nell'utilizzo di un particolare strumento culturale (in risposta alla domanda di ricerca n° 3); la [2] indica il possibile impatto del singolo strumento culturale su uno specifico fattore causa, che a sua volta incide sulla prestazione di sicurezza finale [3] (la relazione [3] esprime cioè l'importanza relativa dei fattori causa per la prestazione di sicurezza e risponde alla prima parte della domanda di ricerca n°5). Le restanti relazioni suppongono invece che gli impatti degli strumenti [4] e dei fattori causa [5] sulle prestazioni di sicurezza possano variare in base ai fattori di contesto, in risposta rispettivamente alla domanda di ricerca n° 4 e 5. Per ricavare invece la risposta alla domanda di ricerca n° 2 basterà combinare le relazioni [2] e [3] e capire dunque l'impatto che ogni singolo strumento ha sulla sicurezza. I fattori di contesto

schematizzati in Figura 57 sono variabili che permettono di distinguere il profilo di un'azienda e si dividono in dimensione (grande, piccola), ambito (strada, ferrovia, entrambe), ruolo nella filiera intermodale (MTO, vettore stradale, gestore del terminal, operatore commerciale del trasporto ferroviario), integrazione verticale (alta, bassa), tipologia di merce trasportata (pericolosa, appetibile, altro) e internazionalizzazione (estesa su scala internazionale, solo Italia).

Passando agli strumenti culturali presi in considerazione dal modello in Figura 57 abbiamo riscontrato come, dall'analisi letteraria riferita alla SCSC, nessun autore abbia mai classificato questa tipologia di strumenti. Abbiamo dunque proposto una classificazione basata su quattro approcci alla security culture, riportata in Figura 58.

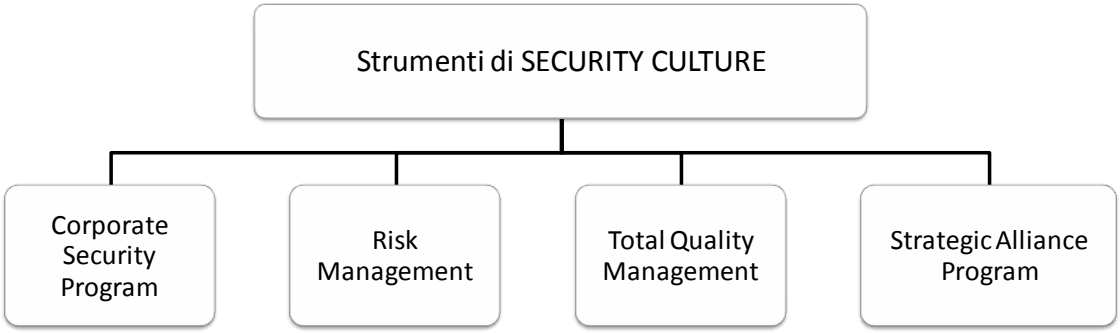


Figura 58: Classificazione degli approcci alla security culture

Nella Tabella 75 è riportato il dettaglio degli strumenti di SCSC individuati.

Tabella 75: strumenti di SCSC

CORPORATE SECURITY PROGRAM	Integrità, lealtà dei dipendenti	investigazione sul passato e colloqui con potenziali dipendenti e terze parti
		programmi di lealtà/fedeltà dei dipendenti
		HR policy
		span of control
	Competenza dei dipendenti sulle tematiche di sicurezza	coinvolgimento esperti esterni
		training dipendenti
		Team work
	Consapevolezza interna sulla sicurezza	assegnazione responsabilità di sicurezza al personale
		sistema di incentivazione e feedback sulla sicurezza
		Punizioni
		programmi di cambiamento organizzativo
		socializzazione informale
		comunicazione interna
		funzione/posizione dedicata alla security (CSO)
	Aspetti soft	simbolismo
		motto
		codice di condotta
RISK MANAGEMENT	Business continuity planning	training dipendenti
		empowerment dei dipendenti
		piani d'azione
	Segnalare incidenti e debolezze	analisi della natura e delle cause degli incidenti (anche minori)
		"Swiss Cheese" model
		monitoraggio dei "near misses"
	Valutazione della conformità di sicurezza	strumenti preventivi di sicurezza basati sull'esperienza reale
		certificazioni
TOTAL QUALITY MANAGEMENT	Partnership	norme di cooperazione
		relazioni di lungo termine
		condivisione di rischi, premi e responsabilità
		sviluppo della fiducia
	Collaborazione tra dipendenti	condivisione di rischi, premi e responsabilità
		teamwork
	Forza lavoro multidisciplinare	interazione cross-funzionale
		assunzione di persone con specifiche competenze
		training dei dipendenti
	Continuous improvement	funzione/posizione dedicata alla security (CSO)
		supporto del top management
		controllo dei processi esistenti
		empowerment dei dipendenti
	Focus sul cliente	-
	Knowledge management	apprendimento inter-aziendale
		istituzionalizzazione della conoscenza
STRATEGIC ALLIANCE PROGRAM	Sviluppo della consapevolezza sulla sicurezza con i miei partner	apprendimento inter-aziendale
		contratti con specifici requisiti di sicurezza
		educazione dei partner
	Riduzione delle differenze di cultura tra azienda e partner	sviluppo della fiducia
		comunicazione esterna
		hibridal cultural interface (HCI)
		socializzazione informale
	Partnership	norme di cooperazione
		relazioni di lungo termine
		Condivisone dei rischi, premi e responsabilità
		sviluppo della fiducia

L'approccio "Corporate Security Program" porta alla definizione di un piano strutturato per lo sviluppo e la diffusione di una cultura della sicurezza in azienda. Gli strumenti che lo costituiscono sono di tipo intra-aziendale e si dividono in programmi di

"**Integrità e lealtà dei dipendenti**" che servono per la selezione e l'affiliazione del personale, "**Competenza dei dipendenti sulle tematiche di sicurezza**" e "**Consapevolezza interna sulla sicurezza**" che agiscono sull'educazione, la formazione e la diffusione delle tematiche di security e gli "**Aspetti soft**" che hanno l'intento di creare una cultura organizzativa capace di influenzare le pratiche di lavoro quotidiano, agendo sulle filosofie, le ideologie, i valori e le aspettative delle persone. Nell'approccio di "Risk Management" sono presenti gli strumenti di stampo culturale che concorrono alla gestione dei rischi e delle vulnerabilità aziendali. Costituiscono questo approccio gli strumenti di "**Business continuity planning**" che descrivono il modo con cui un'organizzazione può far tornare operative le sue funzioni critiche a seguito di una disruption, quelli di "**Segnalazione di incidenti e debolezze**" per l'analisi delle cause degli incidenti/near misses occorsi e quelli di "**Valutazione della conformità di sicurezza**" per il controllo della conformità rispetto a requisiti di sicurezza (prevalentemente riconducibili ai principali programmi di sicurezza volontari). L'approccio di "Total Quality Management" si focalizza sugli strumenti tradizionalmente classificati come "soft TQM". Fanno parte di questo approccio gli strumenti inter-aziendali per l'instaurazione e lo sviluppo di "**Partnership**" e la diffusione di un'ottica di "**Focus sul cliente**" lungo tutta la filiera, e quelli più di stampo intra-aziendale per lo sviluppo della "**Collaborazione tra dipendenti**" e di una "**Forza lavoro multidisciplinare**" per aumentare la resilienza aziendale, oltre al "**Continuous improvement**" e al "**Knowledge management**" per la gestione della conoscenza in ottica di un processo di miglioramento continuo. L'approccio "Strategic alliance program" si focalizza su strumenti di tipo inter-aziendale finalizzati ad ottenere una piena integrazione della filiera intermodale. Ne fanno parte gli strumenti di "**Partnership**" per l'instaurazione di solide relazioni di lungo periodo, quelli di "**Sviluppo della consapevolezza sulla sicurezza con i miei partner**" e di "**Riduzione delle differenze di cultura tra azienda e partner**" che agiscono rispettivamente tramite contratti e training oppure tramite socializzazione informale e sviluppo della fiducia reciproca sulla compatibilità e l'integrazione tra aziende. Su questi 15 strumenti abbiamo focalizzato l'ambito della nostra ricerca, definendo successivamente le prestazioni di sicurezza (e i relativi KPI) su cui questi strumenti possono impattare. Per le prestazioni di sicurezza non abbiamo preso in considerazione solo il focus tradizionalmente analizzato in letteratura, in particolare da Williams et al. (2008) e da IMCOSEC (2010) (corrispondente alla sicurezza di attacchi della Tabella 76), ma

abbiamo preferito avere una visione più ad ampio spettro che comprendesse due differenti filoni di ricerca (da un lato sicurezza preventiva-resilienza, dall'altro attacchi intenzionali-non intenzionali). In Tabella 76 sono schematizzate le prestazioni di sicurezza che abbiamo definito "da attacchi" e "di fornitura".

Tabella 76: Tipologie di sicurezza

	Sicurezza preventiva	**Resilienza**
Attacchi intenzionali	Sicurezza da attacchi	Sicurezza di fornitura
Attacchi non intenzionali		

In linea con IMCOSEC (2010) il KPI scelto per la sicurezza da attacchi è stato il numero di furti/manipolazioni subiti mentre per la sicurezza di fornitura è stato individuato il ritardo subito, il ritardo causato e il ritardo al cliente finale provocato da tutti gli attori della filiera. Inoltre per considerare la relazione causa-effetto che collega gli strumenti ai KPI abbiamo definito dei fattori causa che concorrono a spiegare una cattiva prestazione di sicurezza. Passando infine ad approfondire i fattori causa, per quanto riguarda la sicurezza da attacchi ne abbiamo individuate 3 di possibili cause che possono determinare un furto/manipolazione: episodi collusivi tra persone interne e/o esterne all'organizzazione, errori di qualsiasi natura nell'implementazione di procedure di sicurezza predefinite (errore operativo) ed errori imputabili a chi definisce le procedure e le politiche gestionali (errore di pianificazione). Per i ritardi i fattori causa sono stati individuati in: assenza di collaborazione e comunicazione tra partner di filiera, inadeguatezza dei partner di filiera per lacune presenti nelle procedure/politiche gestionali, ed errori operativi e/o di pianificazione dell'azienda di riferimento.

7.4 Metodologia di ricerca

Definito il modello teorico di riferimento, abbiamo individuato nel caso di studio la metodologia di ricerca da seguire. Il caso di studio, in linea con la natura della nostra ricerca, include dati quantitativi, qualitativi ed elementi teorici e ha l'obiettivo di sviluppare una teoria capace di spiegare i dati raccolti proponendo dei risultati finali di tipo descrittivo (Yin, 2011). Formalmente abbiamo seguito la modalità del caso di studio multiplo (più casi presi in esame) descrittivo (caso sviluppato a valle della definizione del disegno di ricerca) strumentale (funzione di conferma e verifica della

capacità di una teoria pre-esistente di spiegare un determinato fenomeno), in accordo con Yin (2011) e Stake (1995).

In fase preliminare abbiamo delimitato l'unità sulla quale abbiamo concentrato le nostre analisi scegliendo di intervistare un campione d'aziende operante nel settore intermodale il più eterogeneo possibile rispetto ai fattori di contesto individuati. Riferendoci alla Figura 52, abbiamo intervistato 10 MTO, di cui 5 con vettori stradali interni e 7 gestori di terminal intermodale di cui 3 con ulteriore ruolo di operatore commerciale del trasporto ferroviario. Considerata la natura dello studio, abbiamo scelto la modalità dell'intervista personale finalizzata alla compilazione di un questionario per verificare che i manager fossero allineati agli obiettivi del nostro studio. L'intervista si è articolata in un'analisi puntuale di ogni strumento da noi proposto per capirne la tipologia di applicazione in azienda e, in caso di applicazione, le aree d'impatto (positivo o negativo) sulle prestazioni di sicurezza da attacchi e di fornitura. Infine abbiamo rilevato la percezione d'importanza che i manager hanno rispetto agli strumenti proposti, e rispetto ai fattori causa che determinano una cattiva prestazione di sicurezza. Dopo le prime interviste effettuate abbiamo riscontrato quali fossero le difficoltà maggiori per i nostri interlocutori nella compilazione del questionario; sulla base di queste abbiamo accorpato gli strumenti "competenza dei dipendenti sulle tematiche di sicurezza" e "consapevolezza interna sulla sicurezza" in un unico strumento "sviluppo della consapevolezza interna sulla sicurezza" (la differenza tra i due non era infatti percepita) e siamo convenuti nell'utilizzare come unico KPI per la sicurezza di fornitura il "ritardo al cliente finale". Il risultato delle 13 interviste effettuate ci ha consentito di mappare la situazione as-is rispetto all'utilizzo e all'impatto che gli strumenti proposti hanno sulla security aziendale e ci ha fornito la base informativa per consentirci di rispondere alle 5 domande di ricerca.

In Tabella 77 sono riassunte le caratteristiche delle aziende del campione intervistato.

Tabella 77: Campione di aziende intervistate classificate in base ai fattori di contesto

Aziende	Fattori di contesto					
	Dimensione	Ambito	Ruolo	Integrazione verticale	Tipologia di merce	Internazio-nalizzazione
AMBROGIO	grande	strada-ferrovia	MV+GO	alta	A	INT
BAS LOGISTICS	piccola	strada	MV	bassa	A+P	INT
EWALS INTERMODAL	grande	strada	M	bassa	A+P	INT
FERCAM	grande	strada	M	bassa	A+P	INT
HOYER GROUP	grande	strada	MV	bassa	P	INT
HUPAC	grande	ferrovia	GO	alta	A+P	INT
INTERPORTO RIVALTA SCRIVIA	grande	strada-ferrovia	M+G	alta	A+P	INT
MARENZANA	piccola	strada	MV	bassa	P	INT
MAGAZZINI DESIO BRIANZA	piccola	strada-ferrovia	M+G	alta	N	INT
SOGEMAR	grande	strada-ferrovia	MV+GO	alta	A+P	INT
TI.MO.	piccola	ferrovia	G	bassa	A+P	ITA
TERMINALI ITALIA	piccola	ferrovia	G	bassa	A+P	ITA
VOTG	grande	strada	M	alta	P	INT
LEGENDA:	M = MTO, MV = MTO e vettore stradale, G = gestore terminal, GO = gestore terminal e operatore commerciale, P = merce pericolosa, A = merce ad alta appetibilità, N = merce non pericolosa e poco appetibile					

Per il fattore dimensione ci siamo riferiti alla definizione della Commissione Europea 6 maggio 2003, n. 2003/361/Ce; per l'integrazione verticale abbiamo considerato integrate quelle aziende che svolgono almeno un ruolo sia nell'ambito stradale che in quello ferroviario, oppure, nel caso presenti solo in ambito ferroviario, se completamente integrate lato rotaia (G + GO + trazionista ferroviario). Dall'analisi delle caratteristiche del campione abbiamo ritenuto non utile, data la bassa eterogeneità, considerare nello studio di caso due fattori di contesto concentrandoci su dimensione, ambito, ruolo e integrazione verticale.

7.5 Risultati

In riferimento alla prima domanda di ricerca, ossia quali strumenti culturali da noi proposti vengano effettivamente applicati in azienda, si evince come tre strumenti vengano utilizzati molto meno rispetto a tutti gli altri. In Figura 59 è riportato il grafico che, sulla base del campione completo di aziende intervistate, differenzia tutti gli strumenti da noi proposti in termini di utilizzo e importanza percepita dalle aziende.

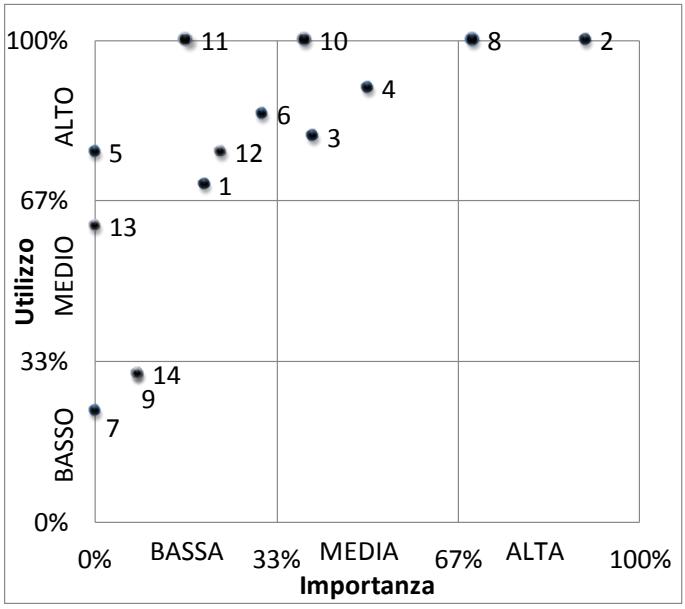


Figura 59: utilizzo/importanza-totale

(1) Forza lavoro multidisciplinare
(2) Collaborazione tra dipendenti
(3) Integrità, lealtà dei dipendenti
(4) Sviluppo della consapevolezza interna sulla sicurezza
(5) Aspetti soft
(6) Continuous improvement
(7) Business continuity planning
(8) Segnalare incidenti e debolezze
(9) Knowledge management
(10) Valutazione della conformità di sicurezza
(11) Partnership
(12) Sviluppo della consapevolezza sulla sicurezza con i miei partner
(13) Riduzione della differenza di cultura tra aziende e partner
(14) Focus sul cliente

Gli strumenti appartenenti al quadrante basso utilizzo-bassa importanza sono: il Business Continuity Planning, per motivi legati alla difficoltà di applicazione nel settore dato il numero troppo elevato di variabili da prevedere e il basso controllo che le aziende possono esercitare sugli altri attori della filiera (in particolare verso il trazionista); il Knowledge Management, di più facile applicazione in settori puramente human intensive e il Focus sul cliente per motivi legati alla natura della filiera intermodale (molto spezzettata) e alla mancanza di un sistema di incentivazione tale da garantire in tutti gli anelli un'attenzione particolare alla buona riuscita dell'intero processo di filiera. In risposta alla seconda domanda di ricerca, cioè capire il possibile impatto che gli strumenti culturali proposti hanno sulle prestazioni di sicurezza, abbiamo creato due mappe causali che evidenziano le relazioni tra strumenti culturali e KPI di sicurezza, passando attraverso gli impatti e i pesi dei fattori causa.

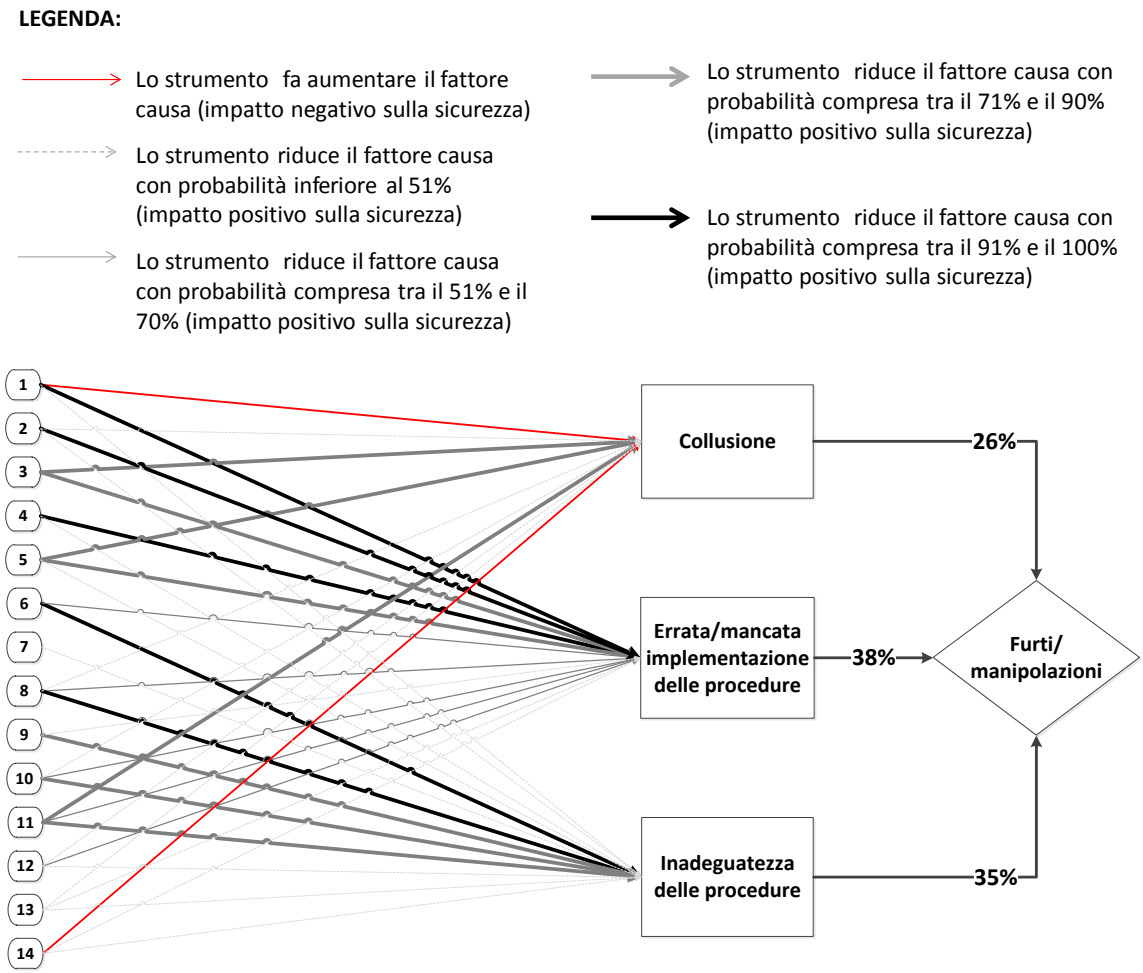


Figura 60: mappa causale-totale-attacchi

Dalla mappa in Figura 60 si evince come le cause dei furti o manipolazioni siano equilibrate. La collusione è quella leggermente meno importante nonostante la forza lavoro multidisciplinare e il focus sul cliente risultino avere impatti negativi su di essa. Questo significa che le aziende riescono a gestire al meglio il trade-off provocato da questi strumenti sulla prestazione di sicurezza. Nonostante molti strumenti abbiano impatti sull'errata e mancata implementazione delle procedure, questa risulta essere la causa principale sulla prestazione di sicurezza da attacchi. In generale, dalle interviste è emerso che le aziende sono ben preparate a limitare episodi di furti e manipolazioni.

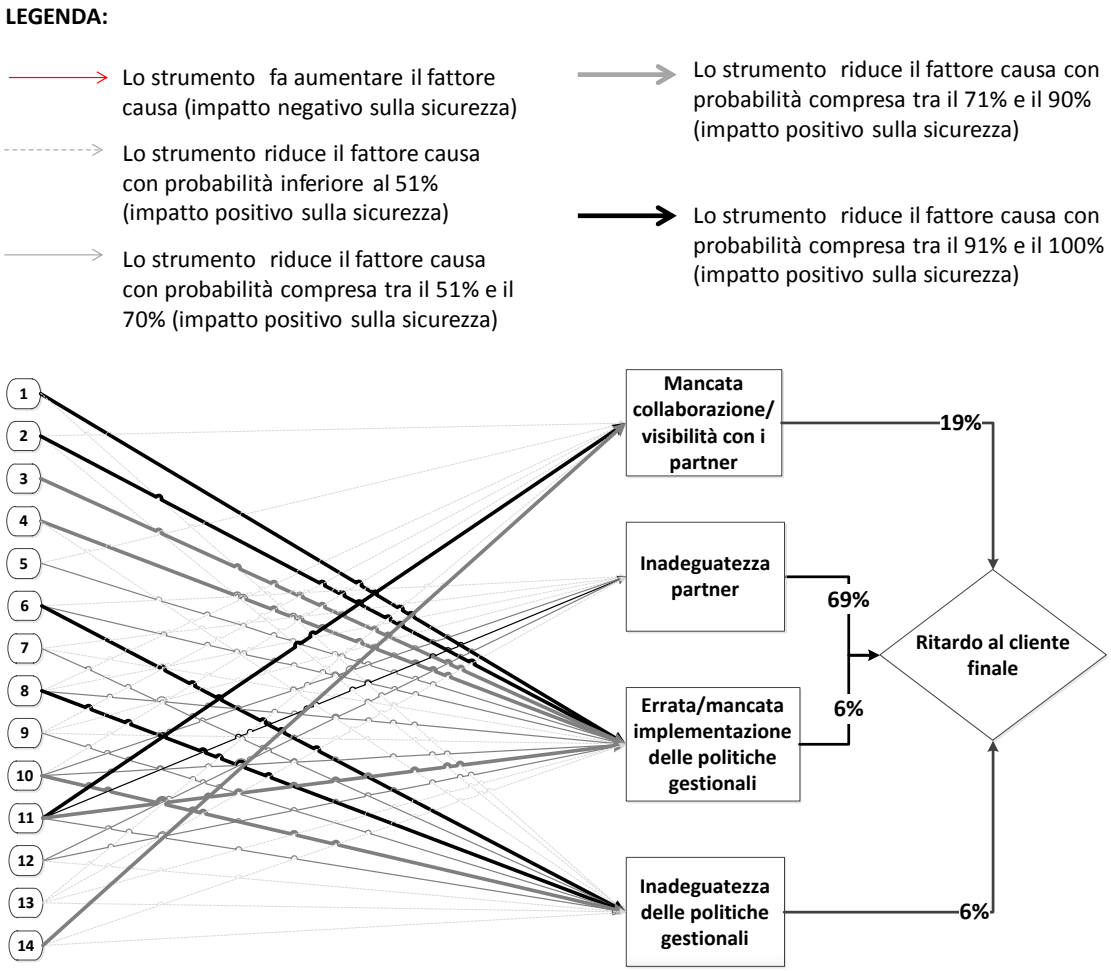


Figura 61: mappa causale-totale-fornitura

Dalla mappa in Figura 61 si evince come il problema principale per le aziende che si occupano di intermodale risieda nel rapporto con i partner di filiera. Analizzando gli impatti degli strumenti si può vedere come questi siano modesti proprio su quei fattori causa "esterni" (mancanza di collaborazione e inadeguatezza del partner) che concorrono maggiormente ad una cattiva prestazione di sicurezza di fornitura. Il motivo risiede nel fatto che è presente una disparità tra l'utilizzo di strumenti interni ed esterni. I primi vengono largamente utilizzati dalle aziende che, per retaggi storici e culturali, sono spinte a focalizzarsi sui processi e le prestazioni interne. Sono presenti invece delle lacune riguardo l'utilizzo di strumenti esterni e questo si traduce in elevati impatti che i fattori causa esterni hanno sulla prestazione finale (per la visione delle diverse mappe causali in funzione dei fattori di contesto si rimanda all'Appendice E).

In relazione alle restanti domande di ricerca abbiamo condotto le medesime analisi suddividendo il campione di aziende in base ai diversi fattori di contesto. I risultati

finali forniscono una panoramica generale sulle differenze di utilizzo degli strumenti culturali proposti in funzione dei diversi fattori di contesto aziendali.

Si denota, come si poteva presumere, che le aziende di dimensioni più elevate sono spinte verso un utilizzo ed una formalizzazione (intesa come standardizzazione della modalità di utilizzo) degli strumenti maggiore (in media vengono applicati dalle grandi aziende 11,75 strumenti su 14 proposti di cui 9,3 in modo formale, mentre per le piccole questo dato scende a 8,2 di cui 4,4 in modo formale). Questo fenomeno è dovuto alla maggiore complessità interna di queste aziende, per le quali risulta difficile poter raggiungere obiettivi di sicurezza senza l'utilizzo formale degli strumenti proposti. Un ulteriore motivo di questa discrepanza tra piccole e grandi aziende risiede nel fatto che la maggior dimensione, con conseguente maggior strutturazione, maggior volume d'affari e maggior potere contrattuale, pone le grandi aziende in una posizione privilegiata nell'applicare gli strumenti proposti.

Per quanto riguarda l'integrazione invece, non c'è una così netta differenza nell'utilizzo degli strumenti proposti (le aziende con alta integrazione applicano in media circa 11 strumenti dei 14 proposti, di cui 8,4 formalmente, contro i 9,57 delle aziende con bassa integrazione, di cui circa 6 formalmente). L'integrazione risulta un fattore discriminante soltanto per due strumenti: la forza lavoro multidisciplinare (anche se spiegata meglio dall'ambito) e il BCP.

Passando al fattore di contesto ambito abbiamo notato come tutti quegli strumenti esterni legati alle prestazioni di filiera vengano maggiormente implementati dalle aziende stradali, il riferimento è in particolare agli strumenti 12-sviluppo della consapevolezza sulla sicurezza con i miei partner, 13-riduzione della differenza di cultura tra azienda e partner e 14-focus sul cliente i quali vengono in media applicati dal 72% delle aziende con interfaccia stradale contro il 33% di quelle ad interfaccia ferroviaria. La motivazione che spinge le aziende ad applicare questi strumenti è la responsabilità sulle prestazione che detengono di fronte al cliente finale; essendo la loro interfaccia, chi lavora in ambito stradale ha sviluppato maggiormente il senso di appartenenza ad un'unica filiera e si impegna nel ridurre le differenze culturali, sviluppare le competenze e la consapevolezza sulle tematiche di sicurezza così da raggiungere elevati target prestazionali (acquisendo così credibilità e fiducia dai clienti industriali). Si nota inoltre un'altra differenza tra le aziende appartenenti ad ambiti diversi. Da un lato le aziende con interfaccia ferroviaria hanno la necessità di impiegare una forza lavoro multidisciplinare (il 67% contro il 33% in ambito stradale), dato

l'elevato numero di mansioni operative svolte all'interno del terminal intermodale (basti pensare ai diversi controlli da effettuare contestualmente all'arrivo e al trasbordo delle ILU); dall'altro le aziende che lavorano in ambito stradale applicano in modo più strutturato e formale gli strumenti legati allo sviluppo delle competenze di sicurezza (100% formale contro il 33% in ambito ferroviario) e alla segnalazione di incidenti (83% formale contro 33% in ambito ferroviario). Questa tendenza è dovuta al fatto che in ambito stradale esiste una maggior variabilità del rischio di incorrere in una disruption rispetto all'ambito ferroviario (in un terminal tutte le attività sono svolte in un unico sito, mentre una società di trasporti su gomma per sua stessa natura svolge le sue attività in siti differenti ed è quindi esposta a maggiori rischi).

Oltre a svolgere le analisi prendendo in considerazione un fattore di contesto per volta, abbiamo ritenuto interessante svolgere un'analisi incrociata combinando tra loro tutti i possibili fattori di contesto ottenendo così otto diversi cluster. Qualsiasi azienda operante nel settore intermodale può quindi essere ricondotta ad uno specifico cluster in funzione dei suoi specifici fattori di contesto. Il risultato di questa analisi incrociata ha portato all'elaborazione di otto diverse check-list di strumenti culturali (in Figura 62 e ra 63) che consentono ad una generica azienda di raggiungere prestazioni di sicurezza (da attacchi e di fornitura) in linea con il settore. Questo non vuol dire avere delle performance di sicurezza ottimali perché, se da un lato le prestazioni del settore sono buone per la sicurezza da attacchi (per le aziende intervistate i furti/manomissioni risultano essere in numero limitato), ciò non è vero per quella di fornitura. Come si evince dalla Figura 61, vi è una netta differenza tra i fattori causa intra-aziendali e quelli inter-aziendali; questo ci suggerisce che il settore presenta una buona sicurezza interna e delle lacune su quella esterna, lasciando elevati margini di miglioramento per quello che riguarda il rapporto con i partner di filiera. Riteniamo che utilizzando in modo più strutturato gli strumenti esterni da noi proposti - che dalle analisi iniziali sul totale del campione risultano i meno utilizzati e ritenuti meno importanti - si possa diminuire in modo significativo il ritardo al cliente finale raggiungendo così una prestazione di sicurezza di fornitura elevata.

Dimensione grande												
Strada						Ferrovia						
alta integrazione verticale			bassa integrazione verticale			alta integrazione verticale			bassa integrazione verticale			
Check-list strumenti per cluster A			**Check-list strumenti per cluster C**			**Check-list strumenti per cluster E**			**Check-list strumenti per cluster G**			
Comuni	2	Collaborazione tra dipendenti	Comuni	2	Collaborazione tra dipendenti	Comuni	2	Collaborazione tra dipendenti	Comuni	2	Collaborazione tra dipendenti	
	3	Integrità, lealtà dei dipendenti		3	Integrità, lealtà dei dipendenti		3	Integrità, lealtà dei dipendenti		3	Integrità, lealtà dei dipendenti	
	5	Aspetti soft		5	Aspetti soft		5	Aspetti soft		5	Aspetti soft	
	6	Continuous improvement		6	Continuous improvement		6	Continuous improvement		6	Continuous improvement	
	8	Segnalare incidenti e debolezze		8	Segnalare incidenti e debolezze		8 (n.f)	Segnalare incidenti e debolezze		8 (n.f.)	Segnalare incidenti e debolezze	
	10	Valutazione della conformità di sicurezza		10	Valutazione della conformità di sicurezza		10	Valutazione della conformità di sicurezza		10	Valutazione della conformità di sicurezza	
	11	Partnership		11	Partnership		11	Partnership		11	Partnership	
Caratteristici	**4**	**Sviluppo della consapevolezza interna sulla sicurezza**	**Caratteristici**	**4**	**Sviluppo della consapevolezza interna sulla sicurezza**	**Caratteristici**	**1**	**Forza multidisciplinare**	**Caratteristici**	**1**	**Forza multidisciplinare**	
	7	**Business continuity planning**		**9 (n.f.)**	**Knowledge management**		**4 (n.f.)**	**Sviluppo della consapevolezza interna sulla sicurezza**		**4 (n.f.)**	**Sviluppo della consapevolezza interna sulla sicurezza**	
	9 (n.f.)	**Knowledge management**		**12**	**Sviluppo della consapevolezza sulla sicurezza con i miei partner**		**7**	**Business continuity planning**		**9 (n.f.)**	**Knowledge management**	
	12	**Sviluppo della consapevolezza sulla sicurezza con i miei partner**		**13**	**Riduzione della differenza di cultura tra aziende e partner**		**9 (n.f.)**	**Knowledge management**	Non utilizzati	7	Business continuity planning	
	13	**Riduzione della differenza di cultura tra aziende e partner**		**14 (n.f.)**	**Focus sul cliente**	Non utilizzati	12	Sviluppo della consapevolezza sulla sicurezza con i miei partner		12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	
	14 (n.f.)	**Focus sul cliente**	Non utilizzati	1	Forza multidisciplinare		13	Riduzione della differenza di cultura tra aziende e partner		13	Riduzione della differenza di cultura tra aziende e partner	
Non utilizzati	1	Forza lavoro multidisciplinare		7	Business continuity planning		14	Focus sul cliente		14	Focus sul cliente	

Figura 62: check-list strumenti culturali per aziende grandi

Dimensione piccola												
Strada						Ferrovia						
alta integrazione verticale			bassa integrazione verticale			alta integrazione verticale			bassa integrazione verticale			
Check-list strumenti per cluster B			**Check-list strumenti per cluster D**			**Check-list strumenti per cluster F**			**Check-list strumenti per cluster H**			
Comuni	2 (n.f.)	Collaborazione tra dipendenti	Comuni	2 (n.f.)	Collaborazione tra dipendenti	Comuni	2 (n.f.)	Collaborazione tra dipendenti	Comuni	2 (n.f.)	Collaborazione tra dipendenti	
	3 (n.f.)	Integrità, lealtà dei dipendenti		3 (n.f.)	Integrità, lealtà dei dipendenti		3 (n.f.)	Integrità, lealtà dei dipendenti		3 (n.f.)	Integrità, lealtà dei dipendenti	
	5 (n.f.)	Aspetti soft		5 (n.f.)	Aspetti soft		5 (n.f.)	Aspetti soft		5 (n.f.)	Aspetti soft	
	6 (n.f.)	Continuous improvement		6 (n.f.)	Continuous improvement		6 (n.f.)	Continuous improvement		6 (n.f.)	Continuous improvement	
	8	Segnalare incidenti e debolezze		8	Segnalare incidenti e debolezze		8 (n.f.)	Segnalare incidenti e debolezze		8 (n.f.)	Segnalare incidenti e debolezze	
	10 (n.f.)	Valutazione della conformità di sicurezza		10 (n.f.)	Valutazione della conformità di sicurezza		10 (n.f.)	Valutazione della conformità di sicurezza		10 (n.f.)	Valutazione della conformità di sicurezza	
	11	Partnership		11	Partnership		11	Partnership		11	Partnership	
Caratteristici	**4 (n.f.)**	**Sviluppo della consapevolezza interna sulla sicurezza**	**Caratteristici**	**4 (n.f.)**	**Sviluppo della consapevolezza interna sulla sicurezza**	**Caratteristici**	**1 (n.f)**	**Forza multidisciplinare**	**Caratteristici**	**1 (n.f.)**	**Forza multidisciplinare**	
	12 (n.f.)	**Sviluppo della consapevolezza sulla sicurezza con i miei partner**		**12 (n.f.)**	**Sviluppo della consapevolezza sulla sicurezza con i miei partner**	Non utilizzati	4	Sviluppo della consapevolezza interna sulla sicurezza	Non utilizzati	4	Sviluppo della consapevolezza interna sulla sicurezza	
	13 (n.f.)	**Riduzione della differenza di cultura tra aziende e partner**		**13 (n.f.)**	**Riduzione della differenza di cultura tra aziende e partner**		7	Business continuity planning		7	Business continuity planning	
Non utilizzati	1	Forza multidisciplinare	Non utilizzati	1	Forza multidisciplinare		9	Knowledge management		9	Knowledge management	
	7	Business continuity planning		7	Business continuity planning		12	Sviluppo della consapevolezza sulla sicurezza con i miei partner		12	Sviluppo della consapevolezza sulla sicurezza con i miei partner	
	9	Knowledge management		9	Knowledge management		13	Riduzione della differenza di cultura tra aziende e partner		13	Riduzione della differenza di cultura tra aziende e partner	
	14	Focus sul cliente		14	Focus sul cliente		14	Focus sul cliente		14	Focus sul cliente	

Figura 63: check-list strumenti culturali per aziende piccole

Come complemento alle check-list, abbiamo inoltre riassunto le best practice che durante le interviste sono emerse riguardo l'applicazione degli strumenti culturali proposti. In ultima istanza abbiamo riassunto i temi trasversalmente riscontrati nel corso delle interviste rispetto alla gestione del servizio intermodale e al suo sviluppo futuro. Questi temi sono:

- il ruolo delle informazioni. Si evince come, oltre ai benefici descritti in letteratura, ci siano anche dei potenziali rischi associati all'aumento di episodi collusivi;
- il vantaggio dell'integrazione verticale. È la tendenza delle più grandi imprese del settore che ne riconoscono i vantaggi in termini di controllo e visibilità sul trasporto end-to-end;
- la focalizzazione del servizio intermodale. Da un lato abbiamo riscontrato una tendenza a differenziare l'offerta di servizi intermodali rispetto alle altre modalità di trasporto per spostare l'attenzione sulle qualità distintive piuttosto che sul mero confronto economico; dall'altro lato la tendenza è quella di specializzarsi su determinate tratte così da ottenere un miglior presidio e un conseguente miglioramento della sicurezza del trasporto;
- la spinta verso la qualità del servizio. Il trasporto intermodale ha degli innegabili vantaggi sulla sicurezza, sull'efficacia e sull'eco-compatibilità. La mancanza di politiche che incentivino queste performance sono allo stato attuale un grosso ostacolo allo sviluppo dell'intermodale.
- la percezione della ferrovia da parte delle industrie e dell'opinione pubblica. Il riferimento è alla situazione italiana che considera la ferrovia come una modalità di trasporto inefficiente e insicura. In realtà il problema è in parte culturale e legato alla tradizione, accentuato da un mancanza di coerenza e di un reale impegno politico per lo sviluppo della ferrovia.

7.6 Conclusioni e sviluppi futuri

Il contributo innovativo del nostro lavoro risiede nell'approfondimento, all'interno del filone di studio della Supply Chain Security, di un'area ancora poco sviluppata riferita alla Supply Chain Security Culture. Abbiamo proposto una classificazione strutturata degli strumenti che concorrono allo sviluppo di questo nuovo approccio alla security che non era presente in letteratura.

La metodologia di analisi scelta è differente da quella utilizzata in riferimento ai classici strumenti di security perché, data la natura degli strumenti culturali, non è possibile proporre un approccio basato semplicemente sul rapporto costi-benefici. Il nostro modello teorico di riferimento, che vuole combinare delle informazioni qualitative e quantitative, può essere generalizzato a qualsiasi azienda del settore intermodale. Attraverso una mappatura della situazione as-is è stato possibile individuare delle specifiche chek-list di strumenti culturali per ogni tipologia di azienda; questo benchmark è utile per allineare le prestazioni aziendali di sicurezza con quelle medie del settore. Abbiamo inoltre individuato le aree di miglioramento di queste prestazioni e le attuali best practice del settore. Il limite del modello proposto è da ricercare nel ristretto campione d'aziende che non permette di effettuare delle analisi statistiche robuste; abbiamo effettuato inoltre delle approssimazioni sui parametri del modello data l'impossibilità di accedere ai dati storici presenti nei database aziendali.

Si evidenzia inoltre come si possa condurre un ulteriore studio complementare che consideri le prestazioni organizzative correlate a quella di sicurezza (come schematizzato in Figura 55). Ad ogni modo lo studio ha permesso di rispondere in modo dettagliato a tutte le domande di ricerca proposte.

Appendice

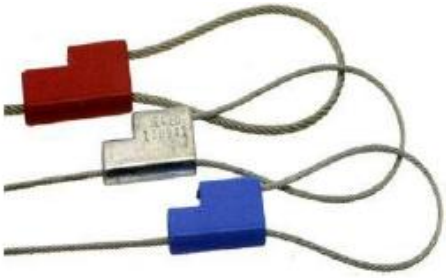
A. Tipologie di sigilli meccanici

Padlock seal

Sigillo di sicurezza di tipo a lucchetto. Corpo in plastica o in metallo e anello con chiusura a morsetto; con o senza chiave.

Cable seal

Cavo con meccanismo di bloccaggio. Richiedono uno strumento per rimuoverli.
Sigillo in un unico pezzo, in cui il meccanismo di chiusura e bloccaggio sono permanentemente attaccati a una estremità del cavo.
Sigillo in due pezzi il cui meccanismo di chiusura separato si infila nel cavo o nella sua estremità.



Bolt seal

Sigillo "perno e bottiglia" composto da un'asta metallica, trattata o non trattata, flessibile o rigida che si infila in una testa con all'estremità una protuberanza e un meccanismo separato di bloccaggio. Richiedono uno strumento per rimuoverli.

Barrier seal

"Sigilli a barra" disegnato e progettato per fornire una barriera significativa all'ingresso del container. Questo sigillo blocca le barre interne di chiusura del container. Può essere riutilizzato

Security seal

Sigilli costruiti con materiali con resistenza all'intrusione molto limitata; è infatti facile rimuoverli. Sono strumento che servono per indicare l'avvenuta manomissione del container.

Indicative seal

Sigilli costruiti con materiale che può essere facilmente rotto a mani nude. Anche questi sigilli servono solo per controllare se il container è stato manomesso.

B. Questionario

Il nostro lavoro di Tesi verte sulla sicurezza nel trasporto intermodale. In particolare l'intervista si focalizzerà sull'analisi di alcuni strumenti per il miglioramento della sicurezza, che abbiamo definito "culturali". Nella seguente tabella abbiamo riportato una breve descrizione per ogni strumento.

Forza lavoro multidisciplinare	Interazioni cross-funzionali, training o coinvolgendo personale con specifica esperienza nei vari ambiti di interesse, con l'obiettivo di aumentare la flessibilità.
Collaborazione tra dipendenti	Lavorare in team condividendo rischi, premi e responsabilità.
Integrità, lealtà dei dipendenti	Strumenti di selezione e di affiliazione del personale, HR policy atte a esplicitare i valori aziendali da perseguire. Possono prevedere azioni per rimediare comportamenti non in accordo con tali valori (ad esempio licenziamento, punizione, training addizionale, etc), oppure azioni volte a premiare la lealtà e fedeltà dei dipendenti (ad esempio premi economici o riconoscimento di status).
Sviluppo della consapevolezza interna sulla sicurezza	Programmi di comunicazione interna, assegnazione di responsabilità su specifiche performance di sicurezza associandole a un sistema di incentivi, coinvolgimento di esperti esterni, istituzione di una figura o funzione aziendale che si occupi a tempo pieno di sicurezza (Chief Security Officer).
Aspetti soft	Aspetti culturali, simbolici, riflessivi e processi di interiorizzazione (ad esempio ideologie, core values, aspettative, comportamenti, tradizioni, motto, codici di condotta).
Knowledge management	Metodologia atta a condividere, formalizzare e rendere disponibile la conoscenza e l'esperienza di ogni persona all'interno dell'azienda.
Valutazione della conformità di sicurezza	Utilizzo di certificazioni/standard e di strumenti addizionali per la prevenzione basati sull'esperienza di incidenti passati e non solo teorici.
Continuous improvement	Processo di cambiamento continuo e incrementale, focalizzato e orientato dal management, ma che vede nelle persone a livello operativo il proprio centro propositivo e propulsivo; effettuato tramite empowerment dei dipendenti, attenzione al controllo dei processi esistenti e supporto del top management.
Business continuity planning	Piani d'azione, training/empowerment dei dipendenti, assicurazioni tali da far tornare operative le funzioni critiche di un'organizzazione entro un predeterminato periodo di tempo

	dopo il verificarsi di una disruption.
Segnalare incidenti e debolezze	Processo di individuazione dei punti deboli, di controllo a più livelli e di analisi degli incidenti e "near misses" volti a imparare e accumulare esperienza. Monitorare "near misses".
Partnership	Relazioni di collaborazione lungo termine, fiducia reciproca, condivisione dei rischi/premi e responsabilità, norme di comportamento comuni con gli altri membri della filiera.
Sviluppo della consapevolezza sulla sicurezza con i miei partner	Diffondere l'importanza delle tematiche di sicurezza attraverso contratti con specifici requisiti e clausole di sicurezza, corsi di formazione al partner oppure conferenze, workgroup con il partner e modelli di apprendimento specifici interaziendali.
Riduzione della differenza di cultura tra aziende e partner	Comunicazione, frequenti rapporti con il partner, sviluppo della fiducia reciproca, adattamento reciproco per ridurre le eventuali differenze/barriere culturali.
Focus sul cliente	Passare da un'ottica locale (di azienda) ad un ottica globale (di filiera) tramite la collaborazione di tutti gli attori della filiera e la realizzazione di un processo integrato.

È opportuno precisare che i benefici che si ottengono da una corretta applicazione di questi strumenti impattano su molteplici prestazioni aziendali (come ad esempio sull'efficienza, sulla qualità, sulla tempestività, etc.). Il nostro intento però, è quello di valutare solo gli impatti che questi hanno sulla sicurezza.

Al termine **sicurezza** attribuiamo due differenti significati:

1. *"Sicurezza da Attacchi"* atta a ridurre la **probabilità** di minacce intenzionali (furti, manomissioni, attacchi terroristici).
2. *"Sicurezza di Fornitura"* atta a ridurre la **probabilità** di minacce non intenzionali (come gli errori umani) e ridurre **l'impatto** della disruption (sia intenzionale che non) così da garantire la continuità del business.

L'obiettivo non è quello di analizzare strumenti che agiscano semplicemente sul normale business (come può essere uno strumento di ottimizzazione dei processi ordinari), ma è quello di focalizzarci su strumenti che facciano ridurre la probabilità di accadimento di una **disruption** (o che ne minimizzino gli impatti). Ad esempio uno strumento che consenta di fronteggiare una forte variabilità della domanda insita nel normale business aziendale non rientra nella nostra analisi, al contrario lo stesso strumento che ci tutela da una variabilità della domanda derivante da una disruprion è di nostro interesse.

Per ogni tipologia di sicurezza abbiamo individuato un KPI sintetico; nello specifico abbiamo considerato:

- il KPI "**Furti/manipolazioni**" (espresso in % rispetto al numero di consegne, in numero di pezzi, in €, in numero di container rubati o manomessi) per la "*Sicurezza da Attacchi"*;
- il KPI "**Ritardo al cliente finale**" (espresso in tempo, in pezzi o in €) per la "*Sicurezza di Fornitura"*.

La prestazione riassunta dal KPI è l'effetto del verificarsi di differenti *"fattori causa"* (collusione, errata/mancata implementazione delle procedure e inadeguatezza delle procedure per il KPI "Furti/manipolazioni"; mancata collaborazione/visibilità con i partner, inadeguatezza partner, errata/mancata implementazione delle politiche gestionali e inadeguatezza delle politiche gestionali per il KPI "Ritardo al cliente finale").

L'obiettivo della nostra intervista è quello di rispondere alle seguenti domande.

- (Per ogni strumento) lo strumento viene utilizzato in azienda? Se no perché?
- (Per ogni strumento) esistono e quali sono gli impatti dello strumento su ciascun fattore causa?
- Quale peso hanno i fattori causa sul KPI? Ad esempio su 100 furti/manomissioni o ritardi è possibile associare una percentuale di incidenza del fattore causa sul KPI o anche solo dare un ordine di importanza relativo?
- Esistono altre ragioni (fattori causa) per cui lo strumento riduce furti/manomissioni o ritardo sul cliente finale?
- Quali sono gli strumenti più importanti?
- Cosa viene misurato in azienda come indicatore di sicurezza?

Queste informazioni ci saranno utili per compilare la tabella seguente.

Importanza			ATTACCHI			FORNITURA			
			FURTI/MANIPOLAZIONI			RITARDO AL CLIENTE FINALE			
		Peso							
		Lo strumento viene utilizzato in azienda?	Collusione	Errata/mancata implementazione delle procedure	Inadeguatezza delle procedure	Mancata collaborazione / visibilità con i fornitori	Inadeguatezza fornitore	Errata/mancata implementazione delle politiche gestionali	Inadeguatezza delle politiche gestionali
	Forza lavoro multidisciplinare								
	Collaborazione tra dipendenti								
	Integrità, lealtà dei dipendenti								
	Competenza dei dipendenti sulle tematiche di sicurezza								
	Sviluppo della consapevolezza interna sulla sicurezza								
	Aspetti soft								
	Continuous improvement								
	Business continuity planning								
	Segnalare incidenti e debolezze								
	Knowledge management								
	Valutazione della conformità di sicurezza								
	Partnership								
	Sviluppo della consapevolezza sulla sicurezza con i miei partner								
	Riduzione della differenza di cultura tra aziende e partner								
	Focus sul cliente								

C. Linee guida per individuare l'utilizzo formale di uno strumento

Nella tabella seguente sono riportate le linee guida da noi utilizzate per stabilire quando uno strumento viene utilizzato formalmente o meno da parte delle aziende intervistate.

Forza lavoro multidisciplinare	• formare il personale non solo sul proprio lavoro ma sul processo in generale
Collaborazione tra dipendenti	• lavoro in team (es. senior con junior o per responsabilità) • sistema di incentivazione/punizione per il team
Integrità, lealtà dei dipendenti	• premi per dipendenti fedeli e leali • policy per comportamento • criteri di selezione del personale
Sviluppo della consapevolezza interna sulla sicurezza	• campagne di comunicazione e riunioni periodiche (con focus sulla security) • sistema di misurazione/incentivi/punizioni sulla sicurezza
Aspetti soft	• motto • codice etico • vision
Knowledge management	• software per la gestione della conoscenza
Valutazione della conformità di sicurezza	• certificazioni/standard • processo di assessment interno/esterno • KPI legati alla sicurezza
Continuous improvement	• incentivazione e programmi di raccolta di idee dal basso • empowerment dei dipendenti
Business continuity planning	• piani d'azione • processi predefiniti da seguire in caso di disruption • empowerment dei dipendenti
Segnalare incidenti e debolezze	• procedura formale di segnalazione • incentivazione ai dipendenti per la segnalazione di near messes
Partnership	• relazioni e contratti di lungo periodo
Sviluppo della consapevolezza sulla sicurezza con i miei partner	• contratti con specifici requisiti e clausole di sicurezza • educazione dei partner e processi di apprendimento specifici inter-aziendali • workgroup con il partner
Riduzione della differenza di cultura tra aziende e partner	• incontri periodici con i partner (anche per la socializzazione) • comunicazione esterna
Focus sul cliente	• sistema di incentivi di filiera

D. Interviste

D.1 Ambrogio

Tipologia azienda: trasportatore specializzato nel traffico intermodale

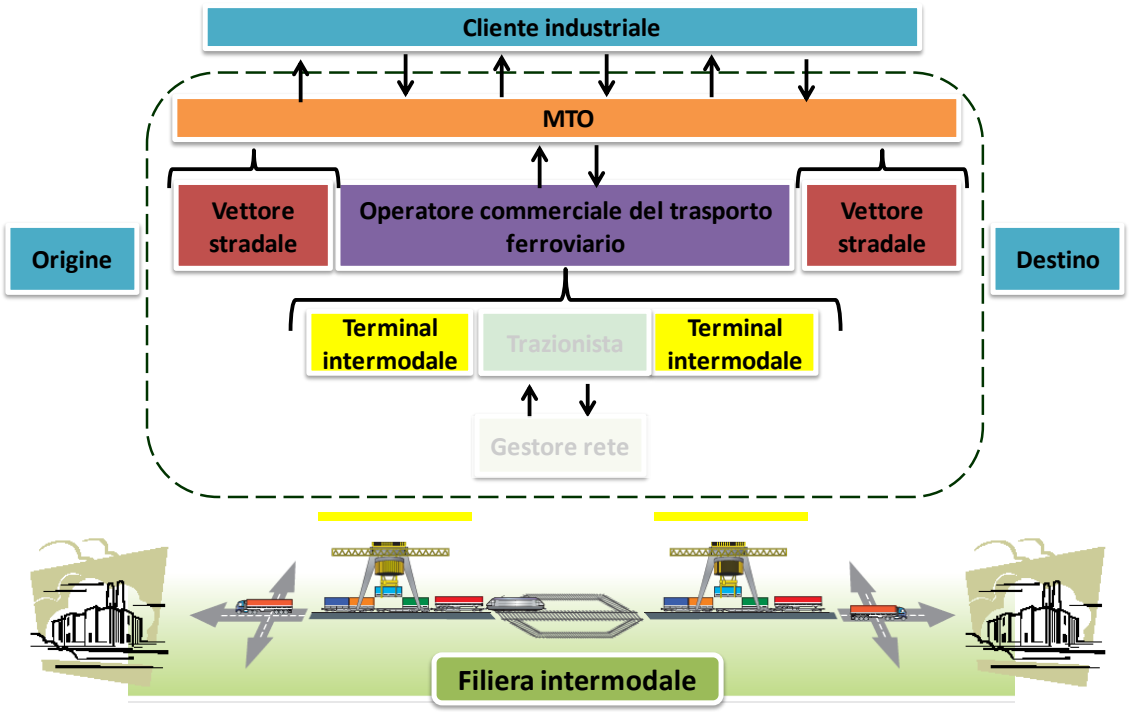
Area di responsabilità diretta: gestione del trasporto su gomma, dello stoccaggio, del terminal intermodale e dell'interfaccia con il cliente finale

Terminal di proprietà: 2 in Italia (Candiolo-Vinovo/Torino e Gallarate/Varese), 2 in Francia (Le Boulou e Mouguerre), 2 in Germania (Neuss e Karlsruhe) e 1 in Belgio (Muizen)).

Fatturato: 80mln € (2009)

Interlocutore: Riccardo Ambrogio, Amministratore Delegato dell'azienda

Sede intervista: Uffici di AMBROGIO TRASPORTI SpA presso il terminal intermodale di Gallarate (VA)



Premessa

AMBROGIO è una società di trasporti fondata nel 1957 da Domenico Ambrogio e una delle prime del settore a porre le basi di moderne strutture di trasporto. Nel 1965 Ambrogio comprese che il trasporto internazionale a lunga distanza non poteva più essere garantito, in termini di costi e di regolarità, unicamente dal trasporto su strada. Questo fece nascere l'idea altamente innovativa dell'integrazione di strada e ferrovia e il passaggio al sistema intermodale. Il Gruppo Ambrogio è costituito da 6 società autonome con sedi in Italia, Francia, Spagna Germania, Belgio e Gran Bretagna dove possiede terminal di proprietà.

L'intervista si è focalizzata sulla gestione della sede di Gallarate che gestisce i flussi di merci tra Italia e Belux, Francia, Gran Bretagna, Irlanda e Germania.

AMBROGIO è una realtà più unica che rara in Italia nel settore del trasporto intermodale; essa è stata infatti la prima impresa italiana ad occuparsi di trasporto intermodale e aveva quindi la necessità di possedere strutture tutte interne all'azienda che si occupassero di ogni aspetto del trasporto (perfino della manutenzione delle casse mobili). A fronte di questa eredità vantaggiosa, AMBROGIO oggi può vantare una logistica molto integrata, tramite i terminal di proprietà con collegamenti privati, i propri dispositivi per la movimentazione delle merci, i depositi e magazzini per la distribuzione, una flotta di casse mobili (oltre 1.300 da 13,6m), carri ferroviari (380 da 2 e 6 assi) e trattori stradali (oltre 200). Mentre la maggior parte delle aziende oggi si rivolgono a terminal pubblici e utilizzano casse mobili di altri.

AMBROGIO essendo l'unica ad avere questa forte integrazione, può vantare elevati differenziali competitivi di qualità.

AMBROGIO si interfaccia con clienti industriali che richiedono un servizio di trasporto a carico completo, occupandosi di tutte le attività dalla presa in consegna della merce presso il deposito del cliente, allo stoccaggio, al trasporto, fino alla consegna puntuale a destinazione.

I partner sono invece chi gli garantisce il trasporto a livello operativo: i trazionisti ferroviari e i padroncini dotati di trattori (i 200 trattori di proprietà non sono sufficienti). Con essi AMBROGIO intrattiene relazioni di lungo termine che, sommati a organizzazione interna, sistemi informativi e avanzati sistemi di comunicazione, conferiscono al Gruppo la capacità di dialogare costantemente col cliente (il quale può conoscere il luogo in cui si trova la propria merce in qualsiasi momento e in tempo

reale). Inoltre, lo stoccaggio e il deposito intermedio garantiscono la consegna delle merci nel luogo previsto e al momento concordato.

La partecipazione che Ambrogio detiene nel capitale azionario del vettore svizzero BLS Cargo ha permesso da un lato di dare un contributo significativo alle strategie della compagnia arricchendola con un punto di vista diverso del mercato; dall'altro lato di apprendere come lavorano le compagnie ferroviarie e quali possano essere i risultati che danno i maggiori vantaggi per entrambe gli attori.

Il Gruppo Ambrogio è costituito da 4 società autonome che gestiscono 7 terminal di proprietà in Italia (Candiolo-Vinovo/Torino e Gallarate/Varese), Francia (Le Boulou e Monguerre), Germania (Neuss e Karlsruhe) e Belgio (Muizen) più altri terminal non di proprietà in Spagna (Barcellona) e Gran Bretagna (Rainham).

L'attività commerciale del Gruppo Ambrogio è costituita per il 50% da scambi con il Benelux e il Regno Unito, il 25% con la Spagna, il 25% con la Germania. Oggi, Ambrogio è uno dei maggiori operatori intermodali in Europa.

A partire dal 1969, da oltre 40 anni, il Gruppo gode di una crescita costante, trasportando in tutta Europa (con oltre 2.300 treni l'anno) le merci di grandi gruppi industriali, soprattutto prodotti chimici, acciaio, generi alimentari e carta. I prodotti ad alto valore sono riconducibili essenzialmente a stampanti da parte i clienti come HP e Epson. Nella realtà i carichi più appetibili (maggiormente soggetti a furti) che l'azienda trasporta sono quelli di tipo alimentare anche rispetto ai carichi completi ad alto valore. Infatti il concetto di appetibilità è ben diverso da quello di alto valore: prodotti alimentari sono più appetibili di un carico di rame perché quest'ultimo sarebbe difficilmente prelevabile e trasportabile.

La nostra intervista si è concentrata sull'operato della sede di Gallarate, la quale si compone di 4 aree:

- un magazzino di 5.000m^2 per lo stoccaggio
- un'officina per la riparazione e manutenzione delle casse mobili
- gli uffici per l'amministrazione e il controllo
- il terminal: area adibita allo scarico/carico merci dai treni che comprende 70.000m^2, 3 binari da 750m, 2 gru a portale e 2 locomotori

Il contributo di Riccardo Ambrogio ci ha sicuramente dato una visione a 360 gradi sull'operato del suddetto terminal.

Adozione degli strumenti

Forza lavoro multidisciplinare

"In Ambrogio sono fortemente presenti gruppi multitask interaziendali. Ciò deriva dal fatto che l'azienda è caratterizzata da una forza lavoro numerosa, se paragonata alle altre aziende del settore, essendo articolata in un numero superiore di aree aziendali".[*]

Come descritto nella premessa, le aree presenti nella sede di Gallarate sono quattro.

La vicinanza fisica di queste aree (come abbiamo potuto constatare visitando la sede di Gallarate) favorisce l'interscambio del personale tra un'area e l'altra, solitamente previsto nelle situazioni di carenza del personale. Tale interscambio determina evidentemente competenze multidisciplinari.

Gli impatti che questa multidisciplinarità genera sui fattori causa della prestazione sicurezza sono i seguenti.

La collusione presenta un trade-off: *"da un lato la presenza di multitask force favorisce la collusione perché ognuno può sapere cosa è arrivato e ci sono maggiori probabilità che vengano date indicazione all'esterno da parte di personale corrotto o interessato al carico. D'altra parte è anche vero che in una realtà così numerosa, se tutti sanno è anche più facile smascherare comportamenti collusivi*".[*]

Per quanto riguarda gli effetti che ha sull'errata/mancata implementazione delle procedure sia lato attacchi che lato fornitura, il nostro interlocutore sostiene che *"il personale che sa tutto potrebbe notare mancanze o dimenticanze di altri".*[*]

Inoltre ha aggiunto che "*il personale ha le competenze sufficienti per mettere in risalto le inadeguatezze nelle procedure anche se opera in un altra area".*[*]

Pertanto si possono ottenere procedure più adeguate dal pun to di vista sia degli attacchi che per la fornitura.

Collaborazione tra dipendenti

"L'interazione tra dipendenti è molto presente in azienda dal momento che si lavora in gruppi di 3 o 4 persone in collaborazione tra loro. Solo nell'area uffici abbiamo 3 team che lavorano sulla gestione degli ordino, sul rapporto con i partner e sul lato import, che non possono essere considerati a se stanti ma uniti da una forte collaborazione".[*]

In termini di impatti ci viene evidenziato lo stesso trade-off emerso dalla multidisciplinarietà, in corrispondenza della collusione. "*Anche lavorare insieme porta*

[*] Frasi estrapolate dall'intervista a Riccardo Ambrogio, Amministratore Delegato di Ambrogio

*le persone a conoscere cosa succede nelle altre aree, indipendentemente dal fatto che alle persone è richiesta una conoscenza multidisciplinare. D'altra parte è più difficile portare avanti comportamenti collusivi, perché è più facile essere mascherati".**

In maniera molto simile alla forza lavoro multidisciplinare, la collaborazione può ridurre l'errata e mancata implementazione delle procedure e l'inadeguatezza delle stesse .

"Il personale che sbaglia di solito è quello nuovo, meno esperto. Quando arriva un'informazione in azienda o un ordine, lavorando fisicamente vicini, l'input arriva a tutto il gruppo di lavoro e quindi il personale più esperto può intervenire. Questo non succede nelle situazioni di lavoro individuale dove è facile lasciare sbagliare le persone.

*Il personale che collabora anche con le altre aree può mettere in risalto inadeguatezze nelle procedure".**

È interessante come la collaborazione tra i dipendenti di Ambrogio, riesca a favorire una maggiore visibilità e controllo sui partner.

*"Nella realtà di Ambrogio i padroncini talvolta è come se fossero dei dipendenti dell'azienda. Lavorando molto vicino può succedere che un traino da effettuare in tale data è a conoscenza di tutti i dipendenti collaboratori, e nel caso in cui ci si accorga che il padroncino non ci sia o non sta effettuando il suo compito, l'azienda se ne può accorgere tempestivamente".**

È un ragionamento molto simile a quello che verrà fatto sulla partnership, ma con una sfumatura leggermente diversa. In questo caso il nostro interlocutore ci fa notare che Ambrogio può accorgersi di un'anomalia o problema del partner anche nel caso di un mancato avviso.

Integrità, lealtà dei dipendenti

*"I provvedimenti disciplinari, la lealtà dei dipendenti, ecc. sono da norma regolati dal contratto di lavoro. In aggiunta l'azienda adotta delle proprie policy aziendali".**

È evidente che queste policy riducono fortemente la collusione perche vanno a combattere comportamenti opportunistici tra dipendenti.

Il nostro interlocutore, a tal proposito, ci ha riportato un esempio su cosa succederebbe se non ci fosse attenzione sull'integrità e lealtà dei dipendenti.

* Frasi estrapolate dall'intervista a Riccardo Ambrogio, Amministratore Delegato di Ambrogio

"Un responsabile potrebbe avere nei confronti del fornitore, comportamenti opportunistici, al fine di appropriarsi del carico; d'altra parte anche il fornitore potrebbe averli nei confronti della parte corrotta dell'azienda, in modo che gli siano concessi ritardi senza punizioni in cambio dei favori concessi. Questa scenario potrebbe far pensare che, oltre ad avere effetti sulla collusione, l'assenza di policy aziendali potrebbero andare a compromettere le prestazioni del fornitore, che non verrebbero più misurate oggettivamente in base ai risultati, ma in base ai favori che fa nei confronti del personale corrotto".[*]

Di conseguenza ci sarebbe un legame, seppur non diretto, tra l'integrità e lealtà dei dipendenti e l'adeguatezza del partner, che proprio per il suo flebile legame abbiamo deciso di non segnarlo come impatto vero e proprio nelle nostre tabelle.

Sviluppo della consapevolezza sulle tematiche di sicurezza

In Ambrogio vengono fatti corsi e riunioni su alcune tematiche di sicurezza, in particolar modo legate al carico. Il nostro interlocutore ci spiega quanto è importante spiegare agli operatori quali siano le procedure da seguire per avere un carico sicuro, a prova ti attacchi o di altri danni. Ad esempio è importante che ogni carico sia legato con delle cinghie particolari.

"Se il lavoratore non è sensibile alle azioni di sicurezza, ad esempio alle azioni preventive per assicurarsi un carico sicuro a prova di ribaltamento tramite lacci e cinghie, il rischio di danni o manipolazioni è alto".[*]

Un esempio che si è verificato, per cui possono esserci procedure adeguate ma non implementate perché non si è consapevoli dell'importanza della procedura stessa, è quello del padroncino che non ha fissato le ruote con i cunei, come da procedura, oltre ad aver inserito il normale freno della motrice, e mentre effettuava lo scarico si è mosso provocando danni. Se tra i lavoratori ci fosse una giusta consapevolezza sulla sicurezza, le procedure verrebbero sicuramente implementate sempre.

"Allo stesso tempo, se l'operatore fosse molto esperto sulle procedure di sicurezza del carico, può segnalare che le procedure messe in atto dall'azienda hanno dei limiti, come è già successo, e proporre un miglioramento delle stesse".[*]

Gli effetti si traducono quindi in una maggiore attenzione nell'esecuzione delle procedure e nel miglioramento delle stesse.

[*] Frasi estrapolate dall'intervista a Riccardo Ambrogio, Amministratore Delegato di Ambrogio

Aspetti soft

Non vengono applicati in azienda. Il motto aziendale ad esempio è più legato all'efficienza e ai benefici in termini ambientali.

In linea teorica, ragionando con il nostro interlocutore sui benefici che potrebbe avere l'adozione di aspetti soft sulla sicurezza, abbiamo ottenuto queste considerazioni:

"Potrebbero avere impatti sull'errata/mancata implementazione delle procedure statement del tipo "zero incidenti nell'ultimo anno", o avvisi che tengono alta l'attenzione dei dipendenti verso le procedure. Attenzione però nell'utilizzo eccessivo di questi strumenti, perché se si esagera si potrebbe finire nell'assurdo. Le cose che si vogliono comunicare potrebbero diventare banali, andando ad intaccare l'autostima dei dipendenti. Poi potrebbe succedere che su nove informazioni banali che vengono comunicate, la decima è di grande importanza, ma i dipendenti non le danno peso. Si ha l'effetto opposto a quello desiderato".[*]

Continous improvement

"Nella sua forma programmata e procedurale, inteso come ricorsi interni, riproposizione di argomenti critici, è normalmente espresso dalle regole aziendali.

Inteso come suggerimenti che partono dal basso è difficilmente riscontrato in azienda, non perché non sia permesso, ma perché i dipendenti non hanno la consapevolezza e voglia di farlo".[*]

È chiaro come in Ambrogio questo strumento - da noi trattato come quel processo di cambiamento continuo e incrementale, orientato dal management, ma che vede nelle persone a livello operativo il proprio centro propositivo e propulsivo - non venga applicato perché mancano le basi, ossia una cultura volta alla segnalazione formale e costante di incidenti, near messes e debolezze.

Business continuity planning

In Ambrogio non ci sono le condizioni necessarie per parlare di Business Continuity Planning, strumento tipico soprattutto delle aziende manifatturiere.

"Il BCP serve essenzialmente quando la catena di comando è lunga. Nel nostro caso, la catena di comando è molto ridotta e l'interconnessione tra capi area e chi vi sta sotto è molto forte. Esistono quindi procedure informali di comunicazione volte a contattare i capi e trovare nell'immediato una soluzione operativa all'anomalia che si è verificata.

[*] Frasi estrapolate dall'intervista a Riccardo Ambrogio, Amministratore Delegato di Ambrogio

Bisogna tenere presente, inoltre, che in questa realtà aziendale è difficile trovare un piano B per il trasporto, data la specificità della merce o del tragitto che deve compiere, e quindi risulta molto difficile stendere un piano formale che garantisca la continuità del business nel caso di imprevisti".[*]

In Ambrogio dunque il BCP viene sostituito dalla possibilità di veicolare le informazioni tempestivamente da chi ha potere decisionale a chi esegue.

Segnalare incidenti e debolezze

In Ambrogio non esiste una pratica formale di segnalazione di incidenti e debolezze, ma laddove l'operatore è disposto a collaborare vengono fatte segnalazioni informali ai propri capi area.

"Ciò è strettamente collegato alla professionalità dell'operatore, ed è il punto in cui trova massima espressione la multidisciplinarietà: i dipendenti tutt'altro che specializzati sul proprio lavoro suggeriscono quando ci sono errori o dimenticanze da parte di altri, e possono offrire la base per individuare inadeguatezze nelle procedure.

I near misses, invece, solitamente vengono comunicati solo quando l'operatore viene coinvolto direttamente nell'incidente, altrimenti è difficile che li segnali".[*]

Questa pratica non sempre viene messa in atto e anche il nostro interlocutore è consapevole che si tratta di una grossa debolezza. Ci è stato infatti riportato un esempio di furto causato da una mancanza dell'operatore che si sarebbe potuto evitare con una segnalazione tempestiva di un incidente.

"Lo dimostra il caso del carico di un noto produttore di alcolici ribaltato in una scarpata lungo l'autostrada, che è stato derubato perché lasciato incustodito durante la notte. In questo caso il padroncino avrebbe dovuto contattare subito l'azienda, la quale avrebbe risposto tempestivamente con delle misure protettive".[*]

Knowledge management

Non esiste un software per la gestione della conoscenza e dell'esperienza. La conoscenza dei capi area viene condivisa formalmente solo all'inizio ai nuovi entranti, tramite corsi per l'inserimento, e poi informalmente tramite corsi interni di aggiornamento, formazione e seminari.

[*] Frasi estrapolate dall'intervista a Riccardo Ambrogio, Amministratore Delegato di Ambrogio

Valutazione della conformità di sicurezza

La valutazione della conformità di sicurezza avviene attraverso un certificatore che periodicamente controlla che tutto sia in regola, e può estendersi anche ai partner dell'azienda.

Ambrogio richiede che vengano fatte delle verifiche periodiche sui padroncini, non solo per verificarne la conformità alle certificazioni nazionali, ma anche per valutare il rispetto del regolamento di Ambrogio e la loro operatività (impatto positivo sull'errata/mancata implementazione delle procedure).

"Questi regolamenti stabiliscono che i partner siano opportunamente certificati, ad esempio, per effettuare trasporti ad alto rischio. Ci aiutano nella scelta di collaboratori adeguati ad ogni specifica esigenza".[*]

Oltre alla influire sull'adeguatezza del partner (nella sua operatività e nelle sue procedure), questo strumento permette di ottenere dei benefici anche applicandolo entro i propri confini aziendali.

"Sicuramente la valutazione periodica della conformità di sicurezza va a risolvere un problema di inadeguatezza delle procedure. Infatti, come è già stato detto, è vero che gli operatori hanno la possibilità di far notare inadeguatezze nelle procedure con una comunicazione bottom up - anche se non sempre lo fanno - , ma il rinnovo delle procedure avviene essenzialmente dall'alto, quindi a seguito delle valutazioni periodiche sulla conformità".[*]

Partnership

Solitamente una solida partnership di lungo periodo non è tipica dei trasportatori intermodali, pertanto si tratta di una peculiarità di Ambrogio e che la rende differenziale agli altri.

Ambrogio possiede terminal di proprietà, e questo gli permettono di tenere sotto controllo tutti i flussi facilmente dato che partono tutti dallo stesso punto. In una situazione del genere è facile e anche più conveniente instaurare partnership con le aziende di traino. Le altre aziende, invece, ricorrono a padroncini sempre diversi e si rivolgono a terminal pubblici.

Una solida partnership ha effetto diretto sulla qualità del servizio. L'influenza positiva della partnership si estende attraverso tutti i fattori causa della prestazione di sicurezza (attacchi e fornitura): riduzione della collusione, degli errori operativi, delle

[*] Frasi estrapolate dall'intervista a Riccardo Ambrogio, Amministratore Delegato di Ambrogio

inadeguatezze nelle procedure e del partner. Ma soprattutto, la partnership permette di risolvere problemi di mancata visibilità e, in alcuni casi, su problematiche di mancata collaborazione con il partner:

"Avendo una forte relazione con il partner, difficilmente rischiamo di lasciare una consegna in bianco, ad esempio per mancanza di padroncini. Se c'è carenza di padroncini, l'azienda partner ci comunica anticipatamente la situazione in modo da poterci riorganizzare. In questo caso abbiamo anche il vantaggio di poter rimediare con mezzi propri". [*]

Riguardo al lato fornitori, la partecipazione che Ambrogio detiene nella società di trasporto ferroviario svizzero, gli permette di apprendere maggiormente come lavorano le compagnie ferroviarie e governare al meglio la relazione con questo anello della filiera.

Sviluppo della consapevolezza sulla sicurezza con i partner

Le iniziative di cui abbiamo parlato riguardo allo sviluppo della consapevolezza interna vengono estese anche ai padroncini esterni di Ambrogio.

"Il padroncino si può definire lavoratore esclusivo di Ambrogio. Se lavora male la responsabilità è di Ambrogio perché è lei che subisce danneggiamenti di immagine. È importante occuparci della loro formazione in prima persona". [*]

Gli impatti sono gli stessi che si ottengono con l'applicazione dello strumento interno analogo.

Riduzione della differenza di cultura tra azienda e partner

Ambrogio incentiva l'allineamento degli obiettivi di medio lungo termine delle due aziende, e allo stesso tempo anche il suo partner ne riconosce il vantaggio.

"Il partner, che ha rapporti esclusivi con Ambrogio, trova convenienza a programmare le sue attività nel medio lungo termine in considerazione agli obiettivi dell'azienda a cui si rivolge. Questo ha effetti più che altro sul medio lungo periodo.

Al di là del contratto c'è un rapporto personale tra i padroncini a conduzione familiare e Ambrogio. I padroncini sono molto integrati, e lavorando insieme da anni ci si fida reciprocamente". [*]

[*] Frasi estrapolate dall'intervista a Riccardo Ambrogio, Amministratore Delegato di Ambrogio

Obiettivi comuni, senso di appartenenza all'azienda del partner e fiducia reciproca sono il risultato di un lavoro continuo di riduzione delle differenze e comportano effetti sulla collusione, inadeguatezza procedure e inadeguatezza del partner.

Focus sul cliente finale

Ambrogio afferma che il focus sul cliente è molto importante.

Ambrogio riesce a muoversi in ottica di soddisfazione del cliente finale sicuramente grazie alla sua forte integrazione lungo la filiera. Infatti, per poter competere nel servizio door to door, è ormai diventato indispensabile saper offrire soluzioni globali su misura per ogni cliente; l'azienda ha la possibilità di rispondere a questa esigenza e riesce a differenziare l'offerta in base ai clienti, come lo dimostra il seguente esempio

"Spesso offriamo servizi su gomma, basti pensare ai casi in cui per emergenza, a causa dello sciopero selvaggio in territorio francese, dobbiamo necessariamente impiegare autocarri per rimediare. O ancora ai territori dell'est europeo, dove l'opzione stradale prevale ancora nettamente da un punto di vista competitivo su quella ferroviaria". [*]

I benefici che si possono ottenere, sono in termini di una migliore visibilità sul cliente stesso e maggiore collaborazione: "*il cliente in qualche modo è sempre sotto i nostri occhi sia direttamente tramite lato commerciale che indirettamente lato padroncini; trattandosi di un ciclo di comunicazione molto breve, il cliente ci informa subito se ci sono problemi, e noi possiamo riorganizzarci per tempo, o migliorare il servizio".*[*]

Tuttavia, una conoscenza approfondita del cliente e del suo carico a volte può comportare effetti negativi sulla sicurezza in termini di collusione.

"Se conosco bene il cliente e quale merce mi consegna, c'è il rischio che si manifestino comportamenti collusivi da parte di chi è interessato al carico". [*]

Una gestione focalizzata sul cliente, dovrebbe prevedere strumenti formali di incentivazione e di misurazione. Sebbene non vengano applicati incentivi di filiera, nel sistema di misurazione vengono però monitorate le prestazioni dei ritardi dovuto a loro e alla ferrovia.

Questo è sufficiente per considerare il focus sul cliente come strumento formale.

[*] Frasi estrapolate dall'intervista a Riccardo Ambrogio, Amministratore Delegato di Ambrogio

Grado di importanza degli strumenti

Tra gli strumenti considerati importanti, vengono evidenziati la collaborazione tra i dipendenti, l'integrità e lealtà, il continuous improvement e lo sviluppo della consapevolezza delle tematiche di sicurezza con i partner.
È interessante il fatto che venga considerato importante uno strumento che in realtà non viene applicato in azienda. Il nostro interlocutore in effetti è consapevole di questo limite e durante l'intervista ci ha fornito una chiara spiegazione su come mai non venga utilizzato: il motivo sta alla radice, in quanto non si tratta di una scelta volontaria da parte di Ambrogio, ma dipende dalla mancanza di volontà dei dipendenti a partecipare a programmi di miglioramento continuo. Questi programmi per il momento rimangono all'interno dei confini del management, e dovrebbero inglobare il contributo e le proposte dei lavoratori, stimolati da un'opportuna incentivazione, per poter dare adito a un vero e proprio processo formale di continuous improvement.

Peso dei fattori causa

Tra i fattori causa che abbiamo proposto, sono stati identificati come i più rilevanti sulla prestazione finale, la collusione per la sicurezza da attacchi, mentre per quanto riguarda la sicurezza di fornitura l'inadeguatezza del partner e la mancata collaborazione/visibilità sempre con il partner, che è quasi sempre l'attore responsabile del ritardo.
"Le prestazioni offerte dipendono inevitabilmente anche dalle compagnie ferroviarie, che troppo spesso hanno rischiato di compromettere la puntualità e l'affidabilità del servizio, e per questo ci sentiamo limitati dall'inefficienza altrui".[*]

Di seguito è riportata la tabella compilata durante l'intervista.

[*] Frasi estrapolate dall'intervista a Riccardo Ambrogio, Amministratore Delegato di Ambrogio

			SICUREZZA DA ATTACCHI			SICUREZZA DI FORNITURA			
			3	2	2	3	3	2	2
		Lo strumento viene utilizzato in azienda?	Collusione	Errata/mancata implementazione delle procedure	Inadeguatezza delle procedure	Mancata collaborazione / visibilità con i partner	Inadeguatezza partner	Errata/mancata implementazione delle politiche gestionali	Inadeguatezza delle politiche gestionali
Forza lavoro multidisciplinare		**f.**	↑↓	↓	↓			↓	↓
Collaborazione tra dipendenti		**f.**	↑↓	↓	↓	↓		↓	↓
Integrità, lealtà dei dipendenti		**f.**	↓						
Sviluppo della consapevolezza interna sulla sicurezza		**f.**		↓	↓			↓	↓
Aspetti soft		**NO**							
Continuous improvement		**NO**							
Business continuity planning		**NO**							
Segnalare incidenti e debolezze		**n.f.**		↓	↓			↓	↓
Knowledge management		**NO**							
Valutazione della conformità di sicurezza		**f.**		↓	↓		↓	↓	↓
Partnership		**f.**	↓	↓	↓	↓	↓	↓	↓
Sviluppo della consapevolezza sulla sicurezza con i miei partner		**f.**	↓	↓				↓	
Riduzione della differenza di cultura tra aziende e partner		**f.**	↓		↓		↓		↓
Focus sul cliente		**n.f.**	↑			↓			

Evidenziati in giallo gli strumenti ritenuti indispensabili per ottenere performance sicure e i principali fattori che causano una minore sicurezza da attacchi e fornitura, la scala utilizzata per i fattori causa è in ordine crescente di importanza.

La risposta "n.f." sull'utilizzo dello strumento in azienda significa che lo strumento viene utilizzato in azienda ma non in maniera standard o formale.

D. 2 Bas logistics

Tipologia azienda: MTO con vettore stradale interno

Area di responsabilità diretta: pianificazione del trasporto intermodale, gestione del rapporto cliente/fornitore e trasporto su gomma

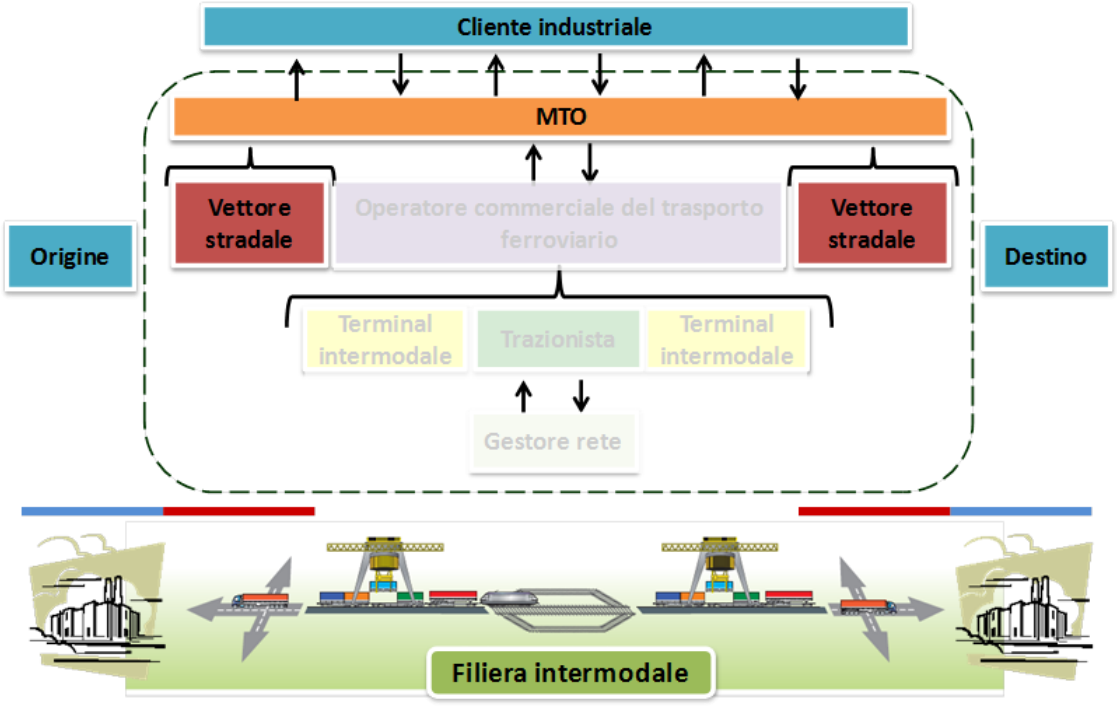
Filiali: Italia e Olanda

Fatturato: 29 mln € (BAS Group, di cui il 10% fornito da trasporto intermodale)

Dipendenti: 210 (BAS Group, di cui il 10% occupato nel settore intermodale)

Interlocutore: Alessandro Negri, Manager Operations

Sede intervista: uffici della BAS logistica Italia presso Cambiago (MI)



Premessa

BAS logistics è un fornitore di servizi di logistica e come espresso nella sua mission "*In una realtà mondiale caratterizzata da rapidi cambiamenti ci presentiamo quali partner affidabili e innovativi in grado di assistervi nel modo più completo con i nostri servizi di trasporto e logistica*".

Il gruppo BAS oltre a BAS logistics comprende Hereijgers BV, un'azienda specializzata in soluzioni di trasporto su misura all'interno del Benelux, e Spoedtransport.nl, azienda specializzata nelle spedizioni urgenti.

BAS possiede una vasta gamma di mezzi per il trasporto stradale (Megatrailer, semirimorchi centinati, semirimorchi refrigerati) e intermodale (casse scarrabili, semirimorchi per treni e container da 45 piedi).

BAS offre la sua gamma di servizi logistici e di trasporto stradale e intermodale con destinazioni in Italia, Spagna, Portogallo, Francia e Benelux.

Con riferimento esclusivamente al trasporto intermodale, BAS si pone come unico interlocutore per il cliente finale nella filiera, curando direttamente la parte di trasporto su strada e affidandosi a partner ferroviari per il cambio di modalità e il trasporto su rotaia.

L'azienda possiede l'intera flotta di trasporto su strada e gli autisti sono tutti dipendenti.

Per quanto riguarda l'Italia, l'azienda si appoggia ai terminal intermodali di Busto Arstizio, Novara, Mortara e Verona con destinazioni prevalentemente nel Benelux.

L'azienda opera nei settori dell'elettronica, del food, della chimica, dei consumer product e dell'industria farmaceutica.

Il contributo di Alessandro Negri offre un punto di vista ad ampio spettro sull'operato di questa azienda logistica.

Adozione degli strumenti

Forza lavoro multidisciplinare

Per quanto riguarda la gestione e formazione della forza lavoro il riferimento è agli autisti.

Questi ricevono una formazione specifica per la loro classe di appartenenza. Tutti gli operatori sono suddivisi in categorie, in particolare due per il trasporto intermodale: autisti di autotreno che trasportano due casse mobili da 7,60 metri, e autisti di bilico, che trasportano casse mobili da 13,60 metri.

L'obiettivo non è quindi quello di diversificare le esperienze nelle varie tipologie di trasporto ma di massimizzare l'esperienza relativa alla singola tipologia di trasporto.

Collaborazione tra dipendenti

La collaborazione interna, sia orizzontale che verticale, è ritenuta un elemento molto importante.

"La collaborazione, intesa come comunicazione e fiducia, è indispensabile per poter fare un buon lavoro".[*]

Per quanto riguarda la collaborazione orizzontale è stata implementata la "politica del mentore".

"Per ogni categoria di autisti, viene indicato un autista come mentore. Questo autista è solitamente quello con più esperienza e diventa anche il responsabile del gruppo. Ogni volta che capita un problema gli altri autisti si rivolgono a lui per chiedere consigli e capire in che modo è meglio procedere. Ad ogni autista mentore viene dato un telefono aziendale per permettergli da un lato di mantenere sempre aperta la comunicazione con gli altri autisti del suo gruppo, e dall'altro di tenere aggiornata la pianificazione e controllo".[*]

La collaborazione verticale è indispensabile per quanto riguarda la definizione del programma giornaliero che gli autisti devono svolgere.

"Molto spesso capita che dopo aver dato il programma agli autisti, loro ci contattino per dare dei consigli sul giro da effettuare. Tutte le decisioni devono in ogni caso essere prese dalla pianificazione ma molto spesso i consigli vengono accettati e viene modificato il giro. Questo tipo di rapporto quotidiano con gli autisti è importante per poter offrire un buon servizio e si ottiene solo con collaborazione, comunicazione e fiducia".[*]

Tutti gli aspetti legati alla collaborazione tra dipendenti sono stati individuati importanti per evitare gli episodi di errata/mancata implementazione delle procedure sia lato attacchi, che lato fornitura.

Integrità, lealtà dei dipendenti

BAS sviluppa delle politiche che premiano la fedeltà e l'integrità dei dipendenti. Esistono degli step precisi per il percorso di ogni dipendente in azienda. Un esempio

[*] Frasi estrapolate dall'intervista ad Alessandro Negri, Manager Operations di BAS Logistics

riferito a queste politiche, è la cerimonia organizzata per i dieci anni di servizio di un autista.

*"Quando un dipendente è da dieci anni in azienda viene organizzata una piccola cerimonia in cui avviene un incontro con il titolare e gli viene conferita una spilla d'oro con un logo che richiama i dieci anni di servizio in azienda. Questo è un modo come un altro che consente di creare un buon clima aziendale, che rafforza i rapporti tra il capo e i dipendenti e che li spinge ad affezionarsi maggiormente all'azienda". **

Queste politiche hanno un impatto, oltre che sulla riduzione degli episodi di collusione del personale, anche sulla motivazione dei dipendenti, spingendoli a svolgere al meglio le loro mansioni quotidiane.

Sviluppo della consapevolezza interna sulla sicurezza

Gli sforzi di BAS di formazione e training dei dipendenti sono rivolti prevalentemente alla sicurezza sul lavoro (safety).

*"Oltre ai corsi di formazione iniziale e quelli obbligatori per la sicurezza sul lavoro, abbiamo fatto a tutti gli autisti un programma di formazione per l'utilizzo di carrelli elevatori e muletti, nonostante sia obbligatorio solo per i magazzinieri. Questo perché nel caso fosse necessario, l'operatore può aiutare nell'effettuare le procedure di carico/scarico in tutta sicurezza". **

Oltre a queste tipologie di formazione vengono periodicamente organizzate delle giornate di training con gli autisti su specifiche tematiche, legate alla sicurezza e non.

*"Aggiorniamo gli autisti con le nuove procedure e segnaliamo quelli che si sono dimostrati dei punti critici del processo. Altri tipi di corsi che abbiamo fatto sono quelli per utilizzare i mezzi con il minor consumo di carburante possibile, o quelli per il trasporto di particolari tipi di merce che deve essere trattata in maniera specifica. In più gli autisti vengono istruiti sull'utilizzo di tutti i nostri dispositivi di sicurezza, dai lucchetti ai sigilli ai dispositivi elettronici presenti sul mezzo".**

Questo tipo di input è utile per far si che vengono effettivamente messe in pratica tutte le procedure per mettere in sicurezza il mezzo, con impatto sulla sicurezza da attacchi intenzionali.

Aspetti soft

BAS è particolarmente attiva per quanto riguarda gli aspetti soft.

* Frasi estrapolate dall'intervista ad Alessandro Negri, Manager Operations di BAS Logistics

È specifica intenzione del proprietario far si che i suoi dipendenti, con particolare riferimento agli autisti, lavorino in un certo modo e si differenzino dai competitor per un servizio sicuro e di qualità.

In azienda è presente il manuale per i dipendenti BAS, strutturato in sei parti : nella prima sono presenti le istruzioni generali, poi una parte riservata agli autisti, una parte relativa al carico e scarico della merce, una parte sulla sicurezza e prevenzione, una parte sul trasporto a temperatura controllata e la parte finale nella quale sono elencati i parcheggi costuditi e i parcheggi vietati, e i numeri telefonici rilevanti.

Oltre alle istruzioni strettamente procedurali, sono molti i richiami all'etica e al comportamento che possa garantire la massima sicurezza. Per esempio viene esplicitata la condotta che devono tenere gli autisti durante le ore di lavoro, oppure i comportamenti per evitare e prevenire i furti di merce.

"Per un'azienda delle nostre dimensioni penso che un manuale scritto di questo tipo sia essenziale sia per quanto riguarda le procedure che i dipendenti devono rispettare, sia per diffondere il modo di lavorare che BAS vuole che i propri dipendenti seguano. Nello specifico poi il nostro manuale è diretto quasi esclusivamente agli autisti e devo dire che per quanto mi riguarda è stato letto e accettato nella maniera giusta". [*]

Oltre al manuale, anche il motto aziendale "BAS top care", scritto sul retro di tutti i mezzi, fa riferimento alla sicurezza e al servizio di qualità che l'azienda vuole offrire.

"Questi aspetti di qualità e sicurezza che l'azienda cerca di trasmettere ai dipendenti, si riscontrano nell'operatività di tutti i giorni. A tutti noi è chiaro qual è la filosofia aziendale e cosa vuol dire lavorare in sicurezza". [*]

In definitiva questa tipologia di strumenti sono ritenuti utili per motivare i dipendenti e migliorare la loro prestazione operativa e per diminuire i casi di collusione, specificatamente trattati nel manuale.

Continous improvement

Bas non ha una politica formale per incentivare le idee e i consigli che arrivano dal lato operativo in ottica di un processo di miglioramento continuo.

È però molto stretta e quotidiana la comunicazione tra gli autisti e la pianificazione, e come accennato precedentemente non è insolito che un autista proponga delle modifiche ai piani delle consegne.

[*] Frasi estrapolate dall'intervista ad Alessandro Negri, Manager Operations di BAS Logistics

"La maggior parte delle volte le indicazioni non sono rivolte alla modifica delle procedure. Le procedure esistenti ci sono, sono standard e precise, e vogliamo che vengano seguite senza eccezioni. Quello che spesso può variare, dopo aver ricevuto il nostro consenso, è il programma degli appuntamenti. Li stimoliamo a darci consigli e suggerimenti, ma non vogliamo che prendano delle iniziative a nostra insaputa". *

Anche per quanto riguarda la sicurezza da attacchi spesso gli autisti danno dei suggerimenti, in particolar modo riguardanti il momento di carico e lo scarico della merce, che è uno di quelli più critici, non tanto per la possibilità di attacchi esterni, ma per furti o negligenze del partner stesso. Non sono rari, infatti, i casi di bolle compilate in modo non chiaro o ambiguo.

Alcuni suggerimenti inoltre, possono sono presi in considerazione anche per il miglioramento delle procedure.

"La filosofia in azienda è che le procedure non saranno mai perfette e sempre migliorabili. L'esperienza, la collaborazione, la comunicazione saranno sempre utili per arrivare a risultati migliori". *

In quest'ottica vengono organizzate periodicamente delle riunioni nelle quali sono presenti i mentori rappresentanti le varie categorie di autisti, il titolare, il responsabile della flotta e il responsabile dell'operativo.

"Questi incontri servono per fare il punto della situazione, parlare dei nuovi problemi emersi e trovare un modo per superarli". *

In aggiunta quando necessario vengono organizzati degli incontri tra i responsabili della filiale italiana e olandese per ottimizzare il coordinamento e le procedure di trasporto.

L'impatto di queste politiche più o meno formali sono state individuate nell'implementazione delle procedure e nel miglioramento delle procedure sia lato attacchi che fornitura.

Business continuity planning

Non esistono piani d'azione prestabiliti da seguire in caso di situazioni impreviste.

"In caso di imprevisti gli autisti sanno che devono contattare immediatamente la pianificazione e insieme cerchiamo di trovare la migliore soluzione alternativa". *

* Frasi estrapolate dall'intervista ad Alessandro Negri, Manager Operations di BAS Logistics

Segnalare incidenti e debolezze

Per quanto riguarda la segnalazione di incidenti la procedura è chiara. Tutti gli autisti sanno che in caso di problemi devono subito avvertire la pianificazione e insieme decidere la soluzione migliore. La comunicazione può essere fatta via telefono o sfruttando il computer di bordo presente su tutti i mezzi.

Infatti tutti i mezzi sono dotati di un sistema satellitare collegato ad un computer di bordo, ed in caso di incidenti o problematiche che causano il fermo del mezzo gli autisti devono immediatamente contattare la pianificazione.

"In pianificazione, grazie al sistema satellitare, ci accorgiamo se un mezzo è fermo o in forte ritardo anche se non abbiamo ricevuto una comunicazione da parte dell'autista. In ogni caso loro sanno che per qualsiasi imprevisto devono subito contattarci così da decidere il da farsi". [*]

Il computer di bordo presenta anche un'opzione che consente agli autisti di segnalare potenziali fonti di pericolo che possono verificarsi durante il trasporto.

"Ovviamente per la segnalazione di queste situazioni molto dipende anche dall'esperienza della persona e dalla sua professionalità. Da solo il sistema informatico non può risolvere tutti i problemi" . [*]

L'impatto di questa politica di comunicazione e della segnalazione dei near messes sono state individuate nell'implementazione delle procedure e nel miglioramento delle procedure stesse sia lato attacchi che fornitura.

Knowledge management

In azienda non è presente un software che formalmente gestisce la conoscenza e la rende disponibile a tutti. Questo processo si attua quotidianamente mediante la collaborazione e la socializzazione informale.

Prima che un mentore lasci il lavoro, gli viene affiancata la persona che andrà a sostituirlo sia durante il lavoro, sia durante le riunioni che si effettuano periodicamente. Questo per permettere a chi subentrerà al mentore di assorbire il più possibile la sua esperienza e il suo modo di lavorare per creare continuità in azienda.

Valutazione della conformità di sicurezza

Bas è molto attiva in ambito certificazioni. Oltre alla ISO 9001, che definisce i requisiti generali per l'implementazione di un sistema di gestione della qualità in azienda, BAS

[*] Frasi estrapolate dall'intervista ad Alessandro Negri, Manager Operations di BAS Logistics

possiede le certificazioni SQAS (Safety and Quality Assessment System), TAPA (Transported Asset Protection Association) e HACCP (Hazard Analysis and Critical Control Points).

La SQAS certifica le procedure applicate in ambito sicurezza, qualità e politiche ambientali, è riconosciuta internazionalmente e viene rilasciata ad aziende che risultano già certificate ISO 9001.

La certificazione TAPA riguarda invece l'ambito del trasporto di merce ad alto valore e si propone di ridurre i furti nelle supply chain internazionali. La certificazione prescrive delle procedure standard, per tutti gli attori della supply chain, progettate per assicurare la sicurezza nel trasporto e nello stoccaggio di merce ad alto valore.

Le certificazioni oltre ad essere un'importante leva di marketing per BAS, sono attualmente, e sono state, determinanti nella progettazione di procedure di trasporto sicure a tutti i livelli. Per esempio sfruttando il network di una delle sue certificazioni, l'azienda è riuscita a progettare, in collaborazione con un operatore ferroviario e con il cliente finale, una linea intermodale per il trasporto di merce che tradizionalmente si movimenta solo su strada.

"Siamo riusciti a combinare con il cliente e con il vettore ferroviario una linea particolare, per fare in modo che la merce durante il trasporto si trovasse in continuo movimento senza pause di stoccaggio intermedio. Questo è stato possibile perché sia noi che il nostro cliente, che l'operatore ferroviario, abbiamo collaborato insieme all`ente preposto alla certificazione al fine di realizzare un progetto comune che permettesse di superare tutti i requisiti imposti dalla certificazione stessa. Per entrambe le parti è stato davvero un successo poter dimostrare che anche il trasporto intermodale, se attuato con determinate procedure, può essere un trasporto veloce e sicuro!". [*]

L'ultima certificazione addizionale, la HACCP riguarda invece il mondo dell'alimentare e prescrive delle procedure per ottenere un controllo igienico sui prodotti, al fine di tutelare la salute dei consumatori.

Gli impatti delle certificazioni in ambito sicurezza da attacchi e di fornitura vanno quindi ricercati nella progettazione di procedure adeguate.

[*] Frasi estrapolate dall'intervista ad Alessandro Negri, Manager Operations di BAS Logistics

Partnership

BAS nell'articolazione della filiera intermodale si appoggia ai terminal di Busto Arsizio, Novara, Mortara e Verona. Il rapporto con questi tutti questi operatori terminalistici è di lungo periodo e basato su una collaborazione continuativa.

Più che da un punto di vista operativo queste relazioni di lungo periodo sono ritenute importanti per la progettazione di linee intermodali sicure, come nell'esempio fatto precedentemente nella valutazione della conformità di sicurezza.

"Per certificare la linea intermodale per merce che tradizionalmente non si trasporta con un sistema combinato strada/ferrovia è stato fondamentale il rapporto esistente con l'operatore del terminal a cui ci siamo appoggiati. I tanti anni di partnership ci hanno infatti permesso di ottenere piena collaborazione e disponibilità per la progettazione della linea. Più volte siamo stati fisicamente dentro il terminal con la persona che si occupava di verificare i requisiti di idoneità, per capire in che modo lavorano e dove c'era bisogno di adeguare le nostre o le loro procedure per ottenere una linea sicura al 100%".[*]

L'impatto della partnership è quindi stato individuato nell'aumento della collaborazione e nella progettazione e implementazione di procedure adeguate sia lato attacchi che fornitura.

Diverso è invece il rapporto con gli operatori ferroviari con i quali c'è solamente un quotidiano scambio di mail e di reportistica sull'andamento del trasporto, che spesso avviene anche in maniera indiretta attraverso l'intermediazione dell'operatore terminalistico.

Sviluppo della consapevolezza sulla sicurezza con i partner

Tutte le azioni di sviluppo della consapevolezza sulla sicurezza non vengono svolte coinvolgendo i partner di filiera ma rimangono all'interno del gruppo BAS.

Riduzione della differenza di cultura tra azienda e partner

Come per le azioni di sviluppo della consapevolezza, anche gli eventi per sviluppare una socializzazione informale rimangono nel perimetro del gruppo BAS e non coinvolgono i partner di filiera.

[*] Frasi estrapolate dall'intervista ad Alessandro Negri, Manager Operations di BAS Logistics

Focus sul cliente finale

Idealmente tutta la filiera dovrebbe lavorare in maniera integrata per assecondare le richieste del cliente finale.

In realtà, essendo la filiera composta da diversi attori, spesso il tornaconto individuale viene messo al primo posto a discapito degli interessi del cliente finale.

"Essendo il punto di riferimento per il cliente, spesso abbiamo a che fare con reclami per problematiche non causate direttamente da noi. Per esempio quando un treno si ferma, non abbiamo alcun margine per intervenire, ma il cliente si rifà su di noi. Ad oggi, per un'azienda come la nostra, è questo il vero limite del trasporto intermodale".[*]

Grado di importanza degli strumenti

Tra gli strumenti analizzati quelli ritenuti indispensabili per ottenere performance sicure sono state la collaborazione tra dipendenti, lo sviluppo della consapevolezza interna sulla sicurezza, la segnalazione di incidenti e debolezze e la valutazione della conformità di sicurezza.

Peso dei fattori causa

Per la sicurezza da attacchi l'inadeguatezza delle procedure è stata individuata come la causa più importante per il verificarsi di un furto o manipolazione. L'errata/mancata implementazione delle procedure è stata individuata come seconda causa e la collusione come un fattore di minor rilievo.

"La mia idea è che quando esistono degli strumenti di controllo e delle procedure totalmente sicure, anche l'intenzione che un dipendente possa compiere un atto volontario per cercare di rubare o manipolare è ridotta ai minimi termini".[*]

Per quanto riguarda la sicurezza di fornitura la mancata collaborazione/visibilità con i partner e l'inadeguatezza del partner sono state individuate come cause principali dei ritardi provocati al cliente finale. L'errata/mancata implementazione delle procedure e l'inadeguatezza delle stesse sono state invece ritenute fattori di minore importanza.

Di seguito è riportata la tabella compilata durante l'intervista.

[*] Frasi estrapolate dall'intervista ad Alessandro Negri, Manager Operations di BAS Logistics

		SICUREZZA DA ATTACCHI			SICUREZZA DI FORNITURA			
		1	2	3	4	4	2	2
	Lo strumento viene utilizzato in azienda?	Collusione	Errata/mancata implementazione delle procedure	Inadeguatezza delle procedure	Mancata collaborazione / visibilità con i partner	Inadeguatezza partner	Errata/mancata implementazione delle politiche gestionali	Inadeguatezza delle politiche gestionali
Forza lavoro multidisciplinare	**NO**							
Collaborazione tra dipendenti	**f.**		↓				↓	
Integrità, lealtà dei dipendenti	**f.**	↓	↓				↓	
Sviluppo della consapevolezza interna sulla sicurezza	**f.**		↓					
Aspetti soft	**f.**	↓	↓				↓	
Continuous improvement	**n.f.**		↓	↓			↓	↓
Business continuity planning	**NO**							
Segnalare incidenti e debolezze	**f.**		↓	↓			↓	↓
Knowledge management	**NO**							
Valutazione della conformità di sicurezza	**f.**			↓		↓		↓
Partnership	**f.**			↓	↓			↓
Sviluppo della consapevolezza sulla sicurezza con i miei partner	**NO**							
Riduzione della differenza di cultura tra aziende e partner	**NO**							
Focus sul cliente	**NO**							

Evidenziati in giallo gli strumenti ritenuti indispensabili per ottenere performance sicure e i principali fattori che causano una minore sicurezza da attacchi e fornitura, la scala utilizzata per i fattori causa è in ordine crescente di importanza.

La risposta "n.f." sull'utilizzo dello strumento in azienda significa che lo strumento viene utilizzato in azienda ma non in maniera standard o formale.

D.3 Ewals intermodal

Tipologia azienda: MTO puro

Area di responsabilità diretta: pianificazione del trasporto intermodale e gestione del rapporto cliente/fornitore

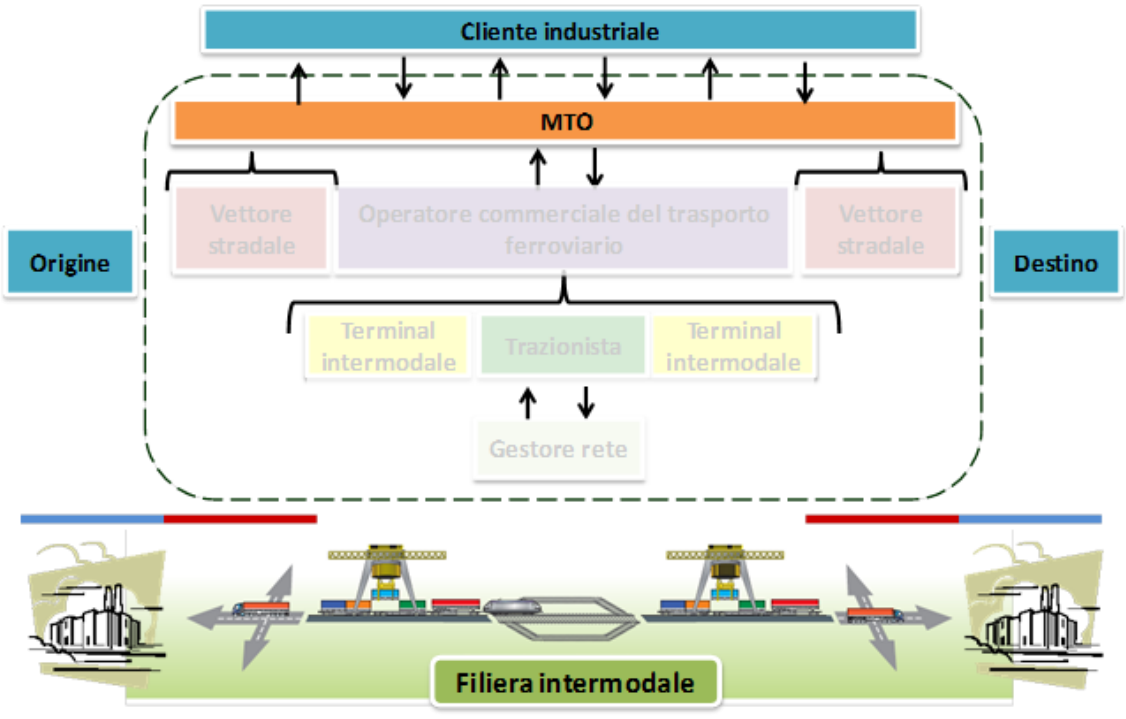
Fatturato: 70 mln € (2010); (395 mln € Ewals Cargo Care)

Dipendenti: 70 (1600 Ewals Cargo Care)

Filiali: Belgio (capogruppo), Italia, Olanda, Germania

Interlocutore: Laura Fortina, Account Manager

Sede intervista: Filiale italiana di Ewals Intermodal c/o l'interporto di Novara



Premessa

Ewals Cargo Care è un'azienda presente con filiali proprie in tutti i principali paesi europei, ed offre l'intera tipologia di servizi logistici (trasporto stradale ed intermodale con flotta propria, varie tipologie di handling e storage, e gestione della flotta altrui per trasporti via strada, rotaia, aereo e nave), con più di cinquant'anni d'esperienza.

Nel 1986 l'azienda ha fondato il primo dipartimento per servizi intermodali, ed a partire dal 2008 ha creato la Business Unit "Ewals Intermodal" con l'obiettivo di differenziare l'offerta di servizi di Ewals Cargo Care per sfruttare al meglio la richiesta di trasporto intermodale.

Ewals Intermodal è diventata completamente autonoma ed operativa dal Giugno 2010 ed attualmente è costituita da 70 dipendenti che gestiscono un traffico medio di 40 treni completi per settimana sulla direttrice Italia – Nord Europa.

Ewals Intermodal è un'azienda di servizi intermodali, che si pone come unico interlocutore con clienti e fornitori della filiera intermodale e supervisiona l'intero processo di trasporto della merce.

Per quanto riguarda la parte operativa del trasporto, Ewals si affida quasi esclusivamente a padroncini esterni per il trasporto su gomma (Ewals Intermodal possiede solo un paio di mezzi di proprietà con autisti dipendenti), ed a operatori terminalistici (in particolare per l'Italia a CIM che gestisce l'interporto di Novara) per il cambio di modalità di trasporto.

Ewals non gestisce direttamente i rapporti con l'operatore ferroviario, compito di competenza dell'operatore terminalistico (in Italia CIM).

Nello specifico i trasporti ferroviari sulla direttrice Italia – Nord Europa vengono effettuati con treni blocco, ovvero motrici che trazionano esclusivamente casse mobili di Ewals.

I 70 dipendenti di Ewals Intermodal si occupano della pianificazione e controllo del traffico intermodale e di tenere i rapporti con fornitori e clienti della filiera.

La tipologia di merce trasportata è molto differente; Ewals serve il settore petrolchimico, automotive, food, ferro, fast consumer goods, high tech, carta e packaging, retail, costruzioni e farmaceutico.

L'azienda ha varie tipologie di ILU di proprietà che vanno dagli Swapbody da 30 e 45 piedi, ai Bulk Container e Container da 30 e 45 piedi, ai Mega Huckepack Trailer e i

Coil Flats da 20 e 25 piedi. Inoltre altre tipologie di equipaggiamento sono rese disponibili da numerose partnership.
Il contributo di Laura Fortina offre un punto di vista non è strettamente operativo, occupandosi in Ewals dell'aspetto commerciale, ma al contrario offre una visione ad alto livello dell'intero processo.

Adozione degli strumenti

Essendo Ewals una società di servizi e non avendo del personale coinvolto operativamente nel processo di trasporto, alcuni degli strumenti proposti non possono essere argomento dell'intervista.

Aspetti soft

Il modo di lavorare in Ewals è molto influenzato dalla cultura base aziendale.
"La mentalità belga/olandese è fortemente incentrata sul lavoro in team e al contrario della mentalità tipicamente italiana i rapporti tra il capo e i membri del team sono quotidiani e molto stretti, e questo si riflette direttamente sul tipo di comportamenti che teniamo durante il lavoro e sulla qualità del servizio che riusciamo ad offrire".[*]
L'importanza degli aspetti soft quali motivazione, motto, ideologie, vision aziendale è testimoniato dalla politica "Heading for Tomorrow" diffusa in tutte le filiale Ewals attraverso veicoli informativi interni e messa in evidenza sul sito della società.
L'iniziativa serve per raccontare il passato e il presente di Ewals, l'evoluzione della società, il modo in cui vuole sviluppare il business e gli scenari di crescita futuri.
"Heading for Tomorrow è lo strumento col quale Ewals vuole trasmettere la sua filosofia di lavoro, incentrata sulla qualità e sulla crescita continua".[*]
Ewals ritiene che progetti come Heading for Tomorrow siano determinanti per creare il "senso di squadra" e per allineare i propri obiettivi con quelli dei partner. Nel concreto tutto questo si traduce in maggiore motivazione degli operatori che lavorano per Ewals, e in crescita della fiducia verso la società.
Il risultato è una migliore prestazione operativa finale ed un approccio più collaborativo alle sfide giornaliere.

Continous improvement

Ewals spinge affinché le aziende partner diano consigli o suggerimenti per rendere il processo più efficiente e sicuro.

[*] Frase estrapolata dall'intervista a Laura Fortina, Account Manager di Ewals

"Vogliamo che i nostri padroncini ci comunichino possibili migliorie di procedure o di gestione del processo. Noi non abbiamo comunicazione diretta con gli autisti; ci aspettiamo però che i loro suggerimenti vengano ascoltati e ci vengano riportati durante i nostri colloqui telefonici o tramite mail".[*]

Non esiste quindi un sistema formale di controllo del processo per l'incentivazione delle idee dal basso; viene però chiesto ai padroncini e agli operatori terminalistici di avere un ruolo attivo e di essere propositivi.

Business continuity planning

In caso di imprevisto durante il trasporto non esistono linee guida formali che prescrivono cosa fare ma la situazione viene valutata al momento dagli addetti alla pianificazione.

"Gli imprevisti possibili sono talmente tanti e vari che non è possibile creare procedure alternative formali. I maggiori imprevisti riguardano la puntualità dei treni in arrivo e partenza e sta ai ragazzi del planning, che sono praticamente disponibili 24 ore su 24, trovare la soluzione migliore per garantire il servizio al nostro cliente finale e modificare le occupazioni degli autisti.

In questi casi cerchiamo anche di capire quali sono i carichi più urgenti da consegnare, ed eventualmente per questi ultimi cerchiamo di approvvigionarci da treni diversi da quelli pianificati, così da evitare situazioni di fermo produzione attribuibili a noi".[*]

Segnalare incidenti e debolezze

Non esiste una procedura formale per trattare le segnalazioni ma comunque queste vengono scambiate nel rapporto corrente con i partner.

"Le segnalazioni non arrivano in forma diretta dall'autista ma tramite il rapporto quotidiano dei colleghi del planning che sono tenuti ad informarci per qualsiasi problematica".[*]

Ewals non ha invece un reale focus sui near messes o un sistema di controllo e gestione delle tipologie di incidenti che si verificano.

Knowledge management

Ewals non possiede un software per la gestione della conoscenza ma la condivisone e lo scambio informativo è un elemento chiave nella gestione quotidiana.

[*] Frase estrapolata dall'intervista a Laura Fortina, Account Manager di Ewals

"Non abbiamo un software per archiviare e gestire la conoscenza. Lo spirito aziendale è però quello di lavorare sempre a stretto contatto e far circolare le informazioni. I nostri capi sono attenti su questo punto e ci hanno inculcato questa mentalità". *

Valutazione della conformità di sicurezza

Ewals richiede che i suoi partner siano certificati e che possiedano le adeguate coperture assicurative.

Nello specifico viene richiesta la certificazione S.Q.A.S (Safety Quality Assessment System) e T.U.V in ambito qualità, ambiente, energia e sicurezza del veicolo di trasporto.

La valutazione della conformità è uno strumento che permette a Ewals di selezionare partner più affidabili sotto l'aspetto strettamente operativo (errata/mancata implementazione delle procedure) e anche sotto l'aspetto dell'integrità del partner (collusione).

Uno dei tanti esempi riferito all'affidabilità operativa del partner può essere il rispetto della procedura imposta agli autisti di non effettuare fermate intermedie durante il trasporto su strada.

Inoltre vengono effettuati controlli periodici dei partner per verificare la sicurezza e la qualità del servizio offerto.

Partnership

Il tratto stradale affidato ai padroncini è il punto della filiera maggiormente esposto agli attacchi intenzionali, in particolare per carichi appetibili come possono essere i carichi di rame.

La partnership è stata individuata come uno strumento efficace per limitare questa tipologia di rischio, in particolare per limitare la collusione e l'errata/mancata implementazione delle procedure.

"I carichi ad alto rischio vengono affidati ai padroncini più affidabili e che hanno degli autisti con maggiore esperienza. Spesso privilegiamo per questo tipo di carichi aziende più piccole, con le quali abbiamo rapporti da molti anni e di cui conosciamo bene gli autisti, piuttosto che affidarci ad aziende più grandi e meno trasparenti. Questo e il controllo fisico e satellitare sul mezzo ci garantisce sicurezza rispetto ai furti e alle manipolazioni". *

* Frase estrapolata dall'intervista a Laura Fortina, Account Manager di Ewals

Rispetto alla totalità del parco fornitori di trasporto su gomma, la maggior parte hanno con Ewals una relazione di lungo periodo. Ogni anno poi possono esserci delle variazioni del parco fornitori dovute a mancati accordi sul prezzo o la tipologia di servizio da offrire.

"Le partnership per noi sono garanzia di qualità del servizio offerto. Abbiamo bisogno di credere nel nostro partner e che i partner credano in noi e per questo avere dei rapporti a lungo termine è fondamentale". *

In generale, la partnership per Ewals non equivale però anche ad una maggiore integrazione e visibilità sull'operato dei padroncini.

"Noi ogni sera diamo il programma dei trasporti che i trazionisti devono effettuare il giorno seguente, ma specialmente con le grosse società non sappiamo chi operativamente eseguirà il servizio. Ci interfacciamo quindi con la ditta di trazione ma non abbiamo il controllo dei mezzi e degli autisti. Questa è una responsabilità dei nostri partner". *

L'interfaccia e la comunicazione tra Ewals e i partner non è differente tra collaboratori spot e collaboratori di lungo periodo. Non esiste un canale preferenziale o comunicazioni privilegiate perché l'obiettivo è *"trattare tutti i trazionisti allo stesso modo e richiedere le medesime prestazioni a tutti i nostri collaboratori".**

Sviluppo della consapevolezza sulla sicurezza con i partner

Oltre alle certificazioni, Ewals impone come precondizione ai potenziali partner un preciso metodo di lavoro che garantisca qualità, efficienza e sicurezza.

Ewals non si impegna però in prima persona nella formazione e training degli operatori, compito che è assegnato alle aziende partner.

Ewals detta quindi le linee guida ma non si pone come l'attore della filiera responsabile della divulgazione e formazione continua sulle pratiche operative e di sicurezza.

Riduzione della differenza di cultura tra azienda e partner

Con cadenza non formalmente definita, Ewals organizza degli incontri con i propri partner con focus sulla sicurezza.

"Ewals organizza dei meeting con le maggiori ditte che offrono servizi di trasporto stradale con lo specifico tema della sicurezza. In questi meeting i nostri responsabili si ritrovano insieme ai responsabili delle ditte di trazione e agli autisti e cercano di far capire al meglio la nostra metodologia di lavoro. Sicuramente queste occasioni sono

* Frase estrapolata dall'intervista a Laura Fortina, Account Manager di Ewals

utili per far crescere la consapevolezza su alcune tematiche di sicurezza per noi fondamentali per poter offrire un servizio di qualità".[*]

Inoltre i meeting organizzati hanno anche l'obiettivo di fortificare il legame esistente, e di creare il senso di squadra che è utile per far diminuire gli episodi di comportamenti opportunistici.

Focus sul cliente finale

Nei meeting con i partner e più in generale nelle quotidiane relazioni di Ewals con i propri interlocutori di filiera, Ewals si pone come promotore dell'idea che tutti gli attori della filiera non possono considerare solo il proprio tornaconto svolgendo unicamente il loro compito, ma deve essere diffusa l'idea di lavorare insieme per un obiettivo comune, ovvero soddisfare il cliente finale.

Questa idea in particolare viene diffusa verso i padroncini, che tra tutti gli attori della filiera sono quelli che maggiormente tendono a concentrarsi esclusivamente sul proprio bene.

"Negli incontri è importante per noi far arrivare ai nostri partner il messaggio che tutti siamo parte di una filiera fatta da tanti attori con responsabilità differenti, e che il lavoro di ogni attore è indispensabile e condiziona anche tutti gli altri".[*]

Pur mantenendo ogni attore la sua area di responsabilità, l'obiettivo è quello di aumentare la collaborazione e la disponibilità reciproca, in particolar modo per gestire le situazioni più critiche.

Per quanto riguarda la possibilità di pensare ad un incentivo di filiera, riconosciuto dal cliente finale e da distribuire a tutti gli attori che riescono a garantire un servizio elevato, è un'ipotesi non più fattibile.

"I clienti nel passato erano più disposti a dare questo tipo di incentivi. Attualmente questa ipotesi non esiste più dato che ormai tutti i clienti pretendono di base un eccellente servizio con costi contenuti. Esistono al contrario le penali da pagare in caso di ritardi e qualsiasi altro tipo di problema, rivolte esclusivamente a noi che siamo il loro unico interlocutore".[*]

[*] Frase estrapolata dall'intervista a Laura Fortina, Account Manager di Ewals

Grado di importanza degli strumenti

Tra gli strumenti analizzati quelli ritenuti indispensabili per ottenere performance sicure sono stati individuati nella valutazione della conformità di sicurezza e nella segnalazione di incidenti e debolezze.
Sono indispensabili perché le certificazioni e i controlli periodici assicurano la qualità del servizio e la segnalazione di incidenti e debolezze è il punto di partenza per il miglioramento del processo.

Peso dei fattori causa

Per quanto riguarda la sicurezza da attacchi :
"Le procedure ci sono e riteniamo che siano sicure. Quando si verifica un furto o una manipolazione solitamente è dovuto alla collusione del personale, essendoci molte persone coinvolte nel processo ed una circolazione non totalmente controllabile delle informazioni. Questo è anche testimoniato dal fatto che i furti spesso sono mirati e rivolti a merce ad alto valore. L'errata o mancata implementazione delle procedure può essere un'altra causa ma di minore rilevanza". [*]
Per quanto riguarda la sicurezza di fornitura :
"La causa principale dei ritardi quando si verifica un evento imprevisto è imputabile all'inadeguatezza del partner. In particolare è imputabile al tratto su rotaia e quindi all'operatore ferroviario. In queste situazioni noi come Ewals non abbiamo la possibilità di proporre soluzioni alternative e ci dobbiamo rimettere ai tempi del trazionista ferroviario.
La secondo causa è imputabile alla mancata collaborazione con i partner con i quali può capitare di non trovare un punto d'accordo per superare una situazione critica.
Per il resto le regole ci sono e sono sicure. Il problema è che esistono talmente tante variabili e situazioni non preventivabili che non è possibile assicurare un servizio puntuale al 100%"[*].

Di seguito è riportata la tabella compilata durante l'intervista.

[*] Frase estrapolata dall'intervista a Laura Fortina, Account Manager di Ewals

		SICUREZZA DA ATTACCHI			SICUREZZA DI FORNITURA			
		3	2	1	3	4	2	1
	Lo strumento viene utilizzato in azienda?	Collusione	Errata/mancata implementazione delle procedure	Inadeguatezza delle procedure	Mancata collaborazione / visibilità con i partner	Inadeguatezza partner	Errata/mancata implementazione delle politiche gestionali	Inadeguatezza delle politiche gestionali
Forza lavoro multidisciplinare								
Collaborazione tra dipendenti								
Integrità, lealtà dei dipendenti								
Sviluppo della consapevolezza interna sulla sicurezza								
Aspetti soft	**SI**	↓	↓		↓		↓	
Continuous improvement	**n.f.**			↓				↓
Business continuity planning	**NO**							
Segnalare incidenti e debolezze	**n.f.**			↓				↓
Knowledge management	**NO**							
Valutazione della conformità di sicurezza	**f.**	↓	↓				↓	
Partnership	**f.**	↓	↓				↓	
Sviluppo della consapevolezza sulla sicurezza con i miei partner	**n.f.**					↓		
Riduzione della differenza di cultura tra aziende e partner	**f.**	↓	↓				↓	
Focus sul cliente	**n.f.**		↓		↓		↓	

Evidenziati in giallo gli strumenti ritenuti indispensabili per ottenere performance sicure e i principali fattori che causano una minore sicurezza da attacchi e fornitura, la scala utilizzata per i fattori causa è in ordine crescente di importanza.

La risposta "n.f." sull'utilizzo dello strumento in azienda significa che lo strumento viene utilizzato in azienda ma non in maniera standard o formale.

D.4 Fercam

Tipologia azienda: MTO puro

Area di responsabilità diretta: pianificazione del trasporto intermodale e gestione del rapporto cliente/fornitore

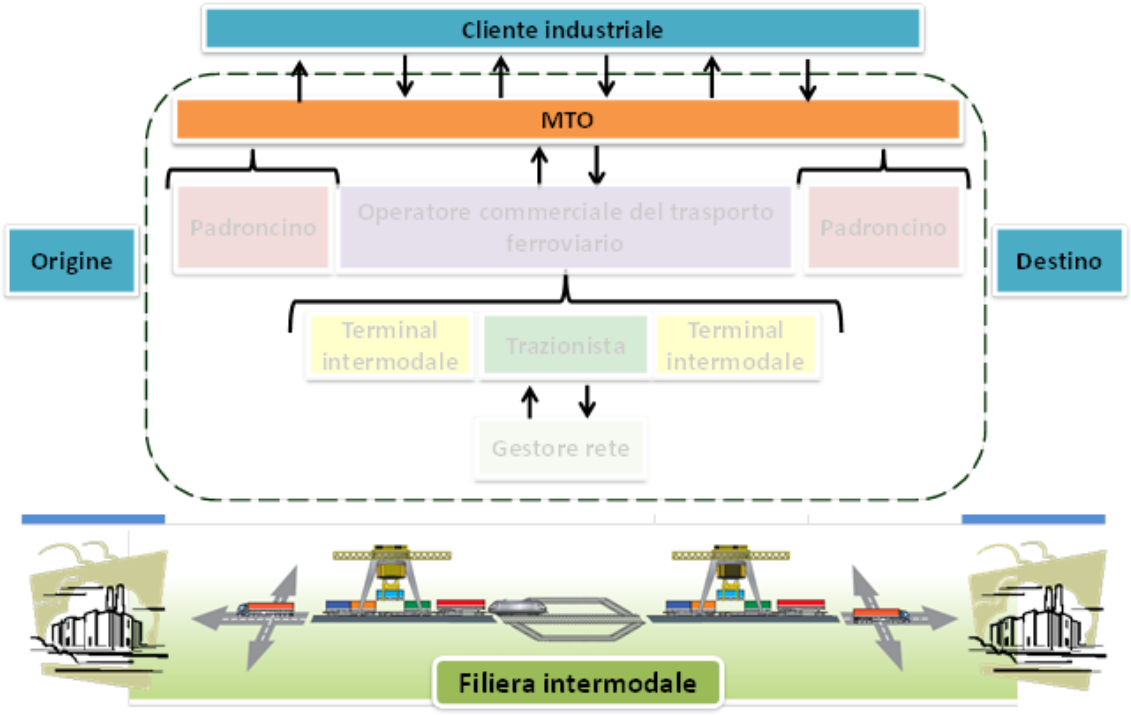
Filiali: 54 (35 in Italia, 18 in Europa, 1 in Marocco)

Fatturato: 430 mln € (2010)

Dipendenti: 1845

Interlocutore: Gianfranco Brillante, Direttore di filiale

Sede intervista: Uffici Fercam c/o la filiale di Rho (MI)



Premessa

Fercam è tra i primi operatori logistici italiani, vanta complessivamente più di 1800 collaboratori in tutta Europa e un parco mezzi di più di 2200 unità di trasporto.

Come espresso nella mission aziendale *"Il nostro contributo primario consiste nella prestazione di servizi logistici a 360° inclusi i processi collegati affinché i nostri clienti possano concentrarsi al massimo sul loro core business. Con i nostri servizi logistici veloci, efficienti ad alto livello qualitativo, informatico e tecnologico, contribuiamo al successo dei nostri partner. Noi contribuiamo allo sviluppo e alla crescita mirata dei collaboratori e siamo garanti della salvaguardia e dell'incremento del benessere sociale. Diamo il nostro contributo ad un mondo ecologicamente intatto facendo particolare attenzione alla parte ecologica nel prestare i nostri servizi".*

Il business aziendale è suddiviso in quattro macroaree:

- Full truck load
- Distribuzione internazionale
- Logistics & distribuzione Italia
- Air & Ocean

All'interno dell'area "Full truck load" l'azienda offre un servizio di tipo intermodale per soddisfare al meglio le esigenze dei clienti industriali che devono effettuare trasporti su lunghe tratte.

Con riferimento esclusivamente al traffico intermodale, Fercam gestisce tratte concentrate tra l'Italia, il Benelux e la Ruhr, paesi dove Fercam è presente direttamente con proprie filiali che consentono un miglior controllo sulla filiera.

L'azienda si appoggia principalmente a terminal intermodali del nord Italia come Busto Arsizio, Milano, Novara, Verona e Padova

Nella sua offerta del servizio strada-rotaia, Fercam sottolinea come con questa tipologia di trasporto venga massimizzata la sicurezza; l'azienda infatti garantisce che la distanza effettuata su gomma (dal terminal al cliente finale) sia al massimo di 200 km così da poter garantire che un giro di consegna e ricarico della cassa mobile avvenga nell'arco di una giornata, evitando nella quasi totalità dei casi soste di veicoli carichi.

A questo proposito le procedure di Fercam impediscono agli operatori di ritirare i contenitori al terminal di sera, posticipando il ritiro al mattino successivo per poterlo consegnare direttamente al cliente in giornata, evitando soste intermedie ed i rischi annessi.

Per quanto riguarda il trasporto vero e proprio, Fercam si appoggia a padroncini esterni per la parte stradale e vettori ferroviari per il cambio di modalità di trasporto e la trazione su rotaia.
L'azienda si occupa esclusivamente della pianificazione e supervisione dell'intero processo di trasporto, ponendosi come unico interlocutore del cliente industriale della filiera.
Il contributo di Gianfranco Brillante offre un punto di vista a 360 gradi sull'operato di uno dei maggiori MTO italiani.

Adozione degli strumenti

Con riferimento al trasporto intermodale, Fercam è una società di servizi, non ha del personale dipendente coinvolto operativamente nel processo di trasporto, ma si occupa esclusivamente della pianificazione, controllo e supervisione. Alcuni strumenti non possono quindi essere argomento dell'intervista.

Aspetti soft

Fercam non ha un codice etico aziendale, però sono diverse le iniziative per i dipendenti che vanno nella direzione di creare un senso di squadra e un buon clima aziendale.
Questa attenzione si può ritrovare nel giornale "WAYS" che Fercam rilascia periodicamente per tutti i propri stakeholder. Il giornale riprende la situazione attuale del business ed i possibili sviluppi futuri ed evidenzia tutte le collaborazioni di successo dell'azienda. Molteplici sono i riferimenti alla qualità del servizio e alla sicurezza, e riprendendo un estratto dal giornale WAYS di Novembre 2010 :
"Confidiamo con l''avvio di questa esperienza editoriale di dare un nostro contributo al miglioramento della cultura presente nel settore ed esaltare quella interna delle risorse umane che operano nel circuito di FERCAM".
Queste iniziative, ancora non facenti parte di una politica formale, sono state ritenute importanti nello sviluppo della cultura aziendale e nella motivazione dei dipendenti, con impatto sui casi di mancata/errata implementazione delle procedure lato attachi.

Continous improvement

Fercam non ha un sistema formale per raccogliere e incentivare i suggerimenti che arrivano dal lato operativo; viene però chiesto ai padroncini di avere un ruolo attivo nell'opera di gestione del rischio e della prevenzione.

"Le comunicazioni di questo tipo avvengono quotidianamente tra la nostra pianificazione e i padroncini. Noi su questa cosa siamo sicuramente attenti e se un autista avanza una proposta intelligente ci attiviamo per fare il possibile. Ovviamente quando affidiamo la trazione ad un padroncino esterno automaticamente responsabilizziamo anche il padroncino, e se il problema sollevato esiste, non riguarda solo noi ma anche lui, visto che comunque ne deve rispondere in prima persona. C'è quindi un doppio livello di attenzione da parte del vettore e da parte nostra che abbiamo in mano la leva della pianificazione. La prevenzione la facciamo in due ".[*]
Questa politica è stata ritenuta impattante sull'adeguatezza delle procedure sia lato attacchi che fornitura.

Business continuity planning

In caso di situazioni impreviste non esistono delle procedure standard prestabilite ma vengono affrontati i problemi di volta in volta.

"Quando ci sono grossi imprevisti come possono essere incidenti che capitano sulla parte ferroviaria, noi siamo completamente in balia dell'operatore ferroviario che a sua volta è in balia del gestore della rete. Se deraglia un treno per esempio, non è l'operatore ferroviario con cui ci interfacciamo che può intervenire, ma chi ha gestisce la struttura delle ferrovie. In quel momento, e in tutta la fase prima e dopo, noi dobbiamo sottostare a chi ha la responsabilità di gestire il problema e l'unica cosa che possiamo fare è informare il cliente industriale sulla base delle informazioni che riceviamo. La mancanza di flessibilità delle ferrovie è il punto più critico del trasporto intermodale".[*]

Segnalare incidenti e debolezze

La segnalazione di incidenti o near messes sono ritenute molto importanti perché sono il primo passo per ottenere un processo di miglioramento continuo delle procedure.

"Per esempio abbiamo vietato di far parcheggiare all'interno dei nostri siti delle casse mobili cariche sganciate dal trattore. Se un mezzo viene parcheggiato all'interno di un sito non si può sganciare il trattore dal rimorchio, per evitare situazioni in cui arriva un altro trattore che aggancia il rimorchio e porta via tutto. Questo è un episodio che sembra strano, ma in passato è capitato, e le nuove procedure sono un esempio di come dalla segnalazione di un pericolo si sia fatto tesoro delle esperienze per definire nuovi

[*] Frasi estrapolate dall'intervista a Gianfranco Brillante, Direttore di filiale Fercam

*accorgimenti per la sicurezza. C'è quindi un'attenzione continua da parte di tutta l'organizzazione, non solo della direzione".**

La procedura per le segnalazioni è formale, e in azienda sono state istituite diverse figure che si occupano esclusivamente di queste problematiche.

*"Abbiamo delle figure che per esempio si occupano della sicurezza della marce, che da noi si chiamano ASM (Assistenza Sicurezza Merce), che hanno come obiettivo quello di creare le condizioni affinchè i rischi siano ridotti al minimo. Nel caso poi succeda qualcosa, loro sono anche gli interlocutori del cliente e del fornitore, e cercano di gestire il problema sia dal punto di vista amministrativo che legale".**

Knowledge management

I traffici intermodali sono gestiti quasi esclusivamente da tre filiali Fercam, tra loro molto integrate e che lavorano su una base software comune.

*"Stiamo elaborando un sistema CRM condiviso tra le filiali, che ha una prospettiva molto più ampia, ma che al suo interno ha anche una parte che serve per la codifica e gestione della conoscenza. Il CRM serve per gestire il rapporto a 360 gradi con il cliente, e ha tra i suoi obiettivi anche quello di gestire tutte le anomalie che nascono nella gestione del servizio intermodale. Quindi consente di avere una statistica di tutte le tipologie di problematiche, di come sono state affrontate e risolte e con quali risultati. Attualmente questo processo lo facciamo in modo informale e non strutturato perché il sistema è ancora in fase di progettazione ma tra qualche tempo sarà pienamente supportato".**

L'impatto di questo strumento è stato individuato nell'inadeguatezza delle procedure sia lato attacchi che fornitura.

*"L'obiettivo ultimo è quello di cercare di sfruttare tutte le informazioni che nascono dal lavoro quotidiano e dagli errori, per correggere le nostre procedure".**

Valutazione della conformità di sicurezza

La valutazione della conformità di sicurezza ha un duplice effetto in Fercam.

Da un lato le certificazioni interne vengono interpretate come un utile strumento per il miglioramento continuo di tutti i processi aziendali, con l'obiettivo di soddisfare in maniera efficace le richieste e le attese del cliente e delle altre parti interessate.

* Frasi estrapolate dall'intervista a Gianfranco Brillante, Direttore di filiale Fercam

L'azienda è certificata ISO 9001 dal 1993 e un'attenzione particolare è stata riservata al sistema di gestione ambientale, certificato ISO 14001 dal 2005.

Dall'altro lato le certificazioni sono uno strumento che l'azienda utilizza per la selezione dei propri partner di filiera, con particolare riferimento ai vettori stradali.

"I nostri vettori partner sono tutti certificati, e soggetti a tutta una procedura per la qualificazione. Il nostro pool di fornitori è piuttosto stabile ed è composto da tutti vettori che hanno passato le nostre procedure di qualità, che analizzano oltre che la parte documentale e amministrativa relativa alle aziende, anche la parte documentale relativa all'autista. Normalmente richiediamo che ci vengano forniti i certificati penali degli autisti per fugare ogni dubbio e abbassare i rischi al massimo". *

La valutazione non è solo fatta in fase di selezione dei partner, ma viene anche fatta in maniera continuativa con ispezioni e controlli.

"Ci sono periodicamente dei controlli che noi facciamo a campione, perché di base ci fidiamo molto della dichiarazione che l'autista fa nel suo lavoro, ma non è sempre detto che ci sia sempre la massima correttezza. Facciamo quindi dei controlli direttamente nei terminal o nei siti di questi padroncini dove andiamo a vedere se le cose corrispondono alle dichiarazioni fatte.

In ogni caso quando partiamo con un nuovo vettore gli assegniamo attività semplici e controlliamo come sul campo opera. Solo dopo averlo controllato siamo tranquilli e lo qualifichiamo, così che possa entrare a far parte dei nostri vettori regolari". *

L'impatto di queste politiche hanno quindi un effetto sulla collusione, diminuendo alla base i rischi di comportamenti poco chiari con una attenta selezione iniziale delle persone oltre che dell'azienda, e sull'errata/mancata implementazione delle procedure e sull'inadeguatezza delle procedure e del partner, sia lato attacchi che fornitura.

Partnership

Le partnership sono ritenute indispensabili per garantire un trasporto di qualità.

Mentre lato ferrovia le relazioni di lungo periodo sono quasi "obbligate" data la situazione di oligopolio che esiste sul mercato, per la parte stradale la partnership è ritenuta indispensabile.

"Cerchiamo sempre di avere dei padroncini relativamente grandi, che abbiano un minimo di strutturazione interna e che non dipendano esclusivamente da noi. I rapporti

* Frasi estrapolate dall'intervista a Gianfranco Brillante, Direttore di filiale Fercam

con questi vettori sono ormai consolidati nel tempo e come orizzonte sono di lungo periodo, dato anche il lungo processo di selezione e controllo".[*]

L'impatto di queste collaborazioni di lungo periodo sono state individuate in prima battuta nella riduzione degli episodi di collusione.

"Sicuramente diminuisce la collusione. Se un padroncino vuole intrattenere un rapporto di lunga durata non può permettersi di avere comportamenti poco chiari. Può capitare, ma se capita il rapporto si interrompe. Diciamo che le partnership sono forse penalizzanti dal punto di vista economico dato l'orizzonte di lungo periodo, dall'altra parte però si trova come beneficio la maggiore attenzione alle procedure e alla soddisfazione reciproca e la sicurezza ne beneficia sicuramente".[*]

Subito dopo l'aspetto legato alla collusione, la partnership garantiscono a Fercam una maggiore possibilità di controllo dei vettori stradali, e la garanzia di avere procedure adeguate per tutto il tratto stradale.

Un altro aspetto legato alle relazioni di lungo periodo, lato ferrovia, è quello di poter ottenere maggiore collaborazione dai partner, soprattutto per quella che è la negoziazione commerciale.

"Capita che il terminal non ci consegni la cassa all'orario previsto. Date le nostre procedure noi se non riusciamo ad organizzare una consegna diretta lasciamo la cassa al terminal fino al giorno successivo. Il rapporto consolidato nel tempo con questi operatori terminalistici ci consente di trovare un punto d'incontro per risolvere la situazione che può essere per esempio farci tenere il contenitore in stoccaggio gratuito nel terminal per la notte. È ovvio che tutte queste negoziazioni risentono positivamente del rapporto consolidato negli anni".[*]

Sviluppo della consapevolezza sulla sicurezza con i partner

Per quanto riguarda il rapporto con i padroncini esterni, Fercam specifica nei contratti oltre ai requisiti più standard come il livello di servizio da garantire e le penali per i furti o ritardi, anche altri parametri che garantiscono la sicurezza a 360 gradi del trasporto.

"La sicurezza non è solo legata al furto della merce o del mancato servizio. La sicurezza per noi è anche come viene caricata la merce, come viene manipolata perché è importante che non subisca danni. Per esempio per la sicurezza delle casse mobili abbiamo previsto che ogni cassa abbia in dotazione 13 cinghie per assicurare che il

[*] Frasi estrapolate dall'intervista a Gianfranco Brillante, Direttore di filiale Fercam

carico sia stabile. L'autista è tenuto a controllare che ogni cassa abbia in dotazione le 13 cinghie e deve comunicarci eventuali mancanze. L'autista è anche tenuto al controllo del carico perché poi per qualsiasi danno che subisce la merce loro ne sono responsabili. È evidente che questa è solo un esempio di procedure che imponiamo e che ci consentono di avere un trasporto fluido e senza intoppi". *

Oltre all'imposizione di procedure, l'azienda opera in prima persona nella formazione e controllo continuo dei suoi padroncini in ottica di un miglioramento continuo del servizio offerto.

"Ci sono delle attività che vengono svolte periodicamente. L'ultima riguardava come fare a legare in sicurezza la merce. Abbiamo fatto intervenire una società tedesca specializzata nella sicurezza stradale. Abbiamo invitato i nostri padroncini e gli abbiamo fatto fare un corso di formazione su come si fa a legare la merce, a seconda del tipo di merce. Abbiamo fatto vedere prima come si deve legare, e poi quali sono gli effetti di un'operazione fatta bene o male. C'è stata prima una formazione teorica nella quale sono stati visionati dei filmati e delle slide, e poi una prova pratica su piazzale per capire cosa succede". *

Dall'altro lato Fercam si interfaccia con operatori ferroviari che impongono determinate procedure agli MTO.

In questo caso è quindi la stessa azienda che deve adattarsi alle richieste degli operatori ferroviari, che devono assicurarsi che i contenitori siano adeguati per poter effettuare il trasporto su rotaia.

"Per esempio c'è stato un periodo nel quale abbiamo avuto diverse segnalazioni dall'operatore ferroviario, perché c'erano delle porte o il telo laterale dei nostri contenitori che si apriva. Dopo due o tre segnalazioni abbiamo cercato di capire quale potesse essere il problema, e dopo aver individuato che era legato a come l'autista bloccava la parete laterale della cassa, abbiamo deciso di fare una sessione di formazione apposita su questa problematica". *

Le casse mobili subiscono quindi un duplice controllo che garantisce ancor di più la sicurezza del trasporto.

* Frasi estrapolate dall'intervista a Gianfranco Brillante, Direttore di filiale Fercam

Riduzione della differenza di cultura tra azienda e partner

Negli incontri periodici con i padroncini, oltre ai momenti di formazione Fercam cerca di organizzare delle attività che aiutino a creare un senso di squadra.
Sono varie tipologie di iniziative che cercano di stimolare la socializzazione informale e la comunicazione e che si rivelano importanti anche ai fini della sicurezza.
Gli impatti sono stati individuati a livello operativo nella riduzione dell'errata/mancata implementazione delle procedure sia lato attacchi che fornitura.

Focus sul cliente finale

Un'azienda come Fercam vive della soddisfazione del cliente industriale della filiera, e cerca quindi di far si che tutti gli attori lavorino con questo stesso obiettivo comune. In realtà questo gli riesce bene soprattutto nella parte su strada del trasporto, nel quale i padroncini esterni sono molto controllati e integrati con l'azienda, mentre diversa è la situazione con gli attori della parte ferroviaria del trasporto che sono molto meno influenzabili.
In ogni caso esistono delle situazioni per cui il cliente industriale riesce a elargire una sorta di incentivo se tutti gli attori della filiera nel complesso lavorano in un certo modo.
"Dipende molto dal tipo di cliente. Alcuni si, anche se l'incentivo non è monetario ma riguarda l'aumento del numero di trasporti che ci affidano se riusciamo a rispettare alcuni parametri. Di solito si mette in piedi un sistema di KPIs e se questi vengono soddisfatti la collaborazione può aumentare. In situazioni di questo tipo rendiamo partecipi anche i nostri fornitori ferroviari di questo fatto. Lo facciamo con tutti i nostri fornitori. È evidente che la nostra qualità di servizio dipende da tutte le maglie, e se ce n'è una che non funziona ne risentono anche tutte le altre. Ovviamente a seconda dell'interlocutore a cui ci rivolgiamo abbiamo leve diverse; se si ragiona con un oligopolista non si può far pressione più di tanto, e il tutto si rifà ad una negoziazione commerciale.
Sistemi di questo tipo ne abbiamo solo con i clienti più grandi e strutturati e che hanno un certo tipo di sistema di controllo della qualità ma non tutti i clienti ci chiedono le stesse cose e seguono queste problematiche con la stessa attenzione. Alla fine direi che comunque non c'è ancora una cultura del trasporto intermodale sviluppata al punto giusto nei clienti industriali; l'aspetto economico è quasi sempre quello determinante".[*]

[*] Frasi estrapolate dall'intervista a Gianfranco Brillante, Direttore di filiale Fercam

Il processo è quindi molto legato alla tipologia di cliente ed è di tipo informale, con impatti sull'inadeguatezza delle procedure sia lato attacchi che fornitura.
Una possibile soluzione alla problematica della poca integrazione delle filiera, l'azienda la sta cercando di risolvere con l'utilizzo di un company train.
"Abbiamo comprato un treno ad una società di trazione ferroviaria che ci mette a disposizione i vagoni, la locomotrice e ci fa la trazione e noi carichiamo tutte le nostre casse su questo treno. Al momento quindi utilizziamo sia gli operatori ferroviari come consolidatori, che il nostro company train, e il miglioramento dal punto di vista della qualità è notevole perché possiamo controllare anche tutta la tratta ferroviaria. Il rischio è ovviamente quello di non riuscire a saturare sempre al meglio il treno".[*]

Grado di importanza degli strumenti

Tra gli strumenti analizzati, quello ritenuto indispensabile per garantire performance sicure è la valutazione della conformità di sicurezza. *"La valutazione della conformità dei nostri partner è fondamentale perché è sempre meglio prevenire che curare. Bisogna sempre sapere con chi si lavora, far implementare le giuste procedure e controllare che siano rispettate per evitare di andare incontro a rischi".* [*]

Peso dei fattori causa

Per quanto riguarda la mancata sicurezza da attacchi il fattore causa principale è stato individuato nella collusione, seguito dall'errata/mancata implementazione delle procedure e dall'inadeguatezza delle procedure considerate allo stesso livello.
"La collusione è sempre la prima causa alla quale si pensa. Poi a volte si può pensare solo male, però quanto capita un furto guarda caso è sempre merce di valore. La collusione può anche essere al di fuori di quello che è il nostro ambito di responsabilità, perché può venire dal magazzino del cliente stesso o comunque essere esterna all'ambito del trasporto e quindi difficilmente controllabile".[*]
Per quanto riguarda la mancata sicurezza di fornitura l'inadeguatezza del partner è stata individuata come primo fattore causa, seguita dalla mancanza di collaborazione/visibilità con il partner e successivamente dalle mancanze operative e delle politiche gestionali.
Di seguito è riportata la tabella compilata durante l'intervista.

[*] Frasi estrapolate dall'intervista a Gianfranco Brillante, Direttore di filiale Fercam

		SICUREZZA DA ATTACCHI			SICUREZZA DI FORNITURA			
		3	2	2	3	4	2	2
	Lo strumento viene utilizzato in azienda?	Collusione	Errata/mancata implementazione delle procedure	Inadeguatezza delle procedure	Mancata collaborazione / visibilità con i partner	Inadeguatezza partner	Errata/mancata implementazione delle politiche gestionali	Inadeguatezza delle politiche gestionali
Forza lavoro multidisciplinare								
Collaborazione tra dipendenti								
Integrità, lealtà dei dipendenti								
Sviluppo della consapevolezza interna sulla sicurezza								
Aspetti soft	**n.f.**		↓					
Continuous improvement	**n.f.**			↓				↓
Business continuity planning	**NO**							
Segnalare incidenti e debolezze	**f.**			↓				↓
Knowledge management	**n.f.**			↓				↓
Valutazione della conformità di sicurezza	**f.**	↓	↓	↓		↓	↓	↓
Partnership	**f.**	↓		↓	↓	↓		↓
Sviluppo della consapevolezza sulla sicurezza con i miei partner	**f.**		↓	↓		↓	↓	↓
Riduzione della differenza di cultura tra aziende e partner	**f.**		↓				↓	
Focus sul cliente	**n.f.**			↓				↓

Evidenziati in giallo gli strumenti ritenuti indispensabili per ottenere performance sicure e i principali fattori che causano una minore sicurezza da attacchi e fornitura, la scala utilizzata per i fattori causa è in ordine crescente di importanza.

La risposta "n.f." sull'utilizzo dello strumento in azienda significa che lo strumento viene utilizzato in azienda ma non in maniera standard o formale.

D.5 Hoyer Group

Tipologia azienda: MTO e azienda di trasporto specializzata in bulk logistic.

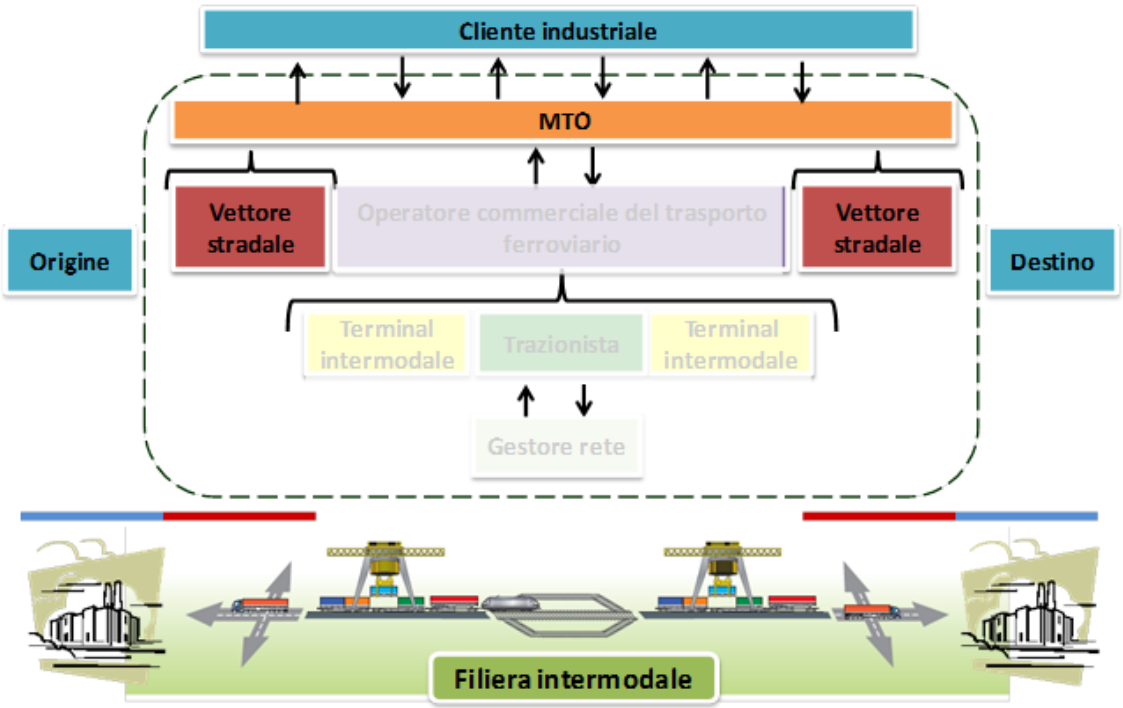
Area di responsabilità diretta: pianificazione del trasporto intermodale, noleggio container e gestione del rapporto cliente/fornitore,

Fatturato: 987 mln €

Dipendenti: 5200

Interlocutore: Sabrina Robba, Managing Director di HOYER Italia S.r.l. e di HOYER Svizzera SA e responsabile della sicurezza, ambiente e qualita' di tutto il gruppo HOYER

Sede intervista: sede di HOYER (Svizzera) SA Mendrisio (CH)



Premessa

HOYER Group, colosso tedesco fondato nel 1946, è leader in Europa nella logistica di prodotti liquidi chimici, alimentari, gas e prodotti petroliferi, e secondo operatore logistico di tank container in tutto il mondo, ed è capace di produrre un giro d'affari di 990 milioni di euro e di impiegare circa 5.200 persone.

HOYER si appoggia alla modalità di trasporto intermodale per distribuire un'ampia gamma di container in tutto il mondo via strada, ferrovia e mare. Dotato di una flotta di 22.800 tank container nel 2010, tra cui road container e IBC (Intermediate Bulk Container), e 3.100 trailer, è in grado di rispondere a qualsiasi esigenza del cliente e richiesta di personalizzazione del trasporto.

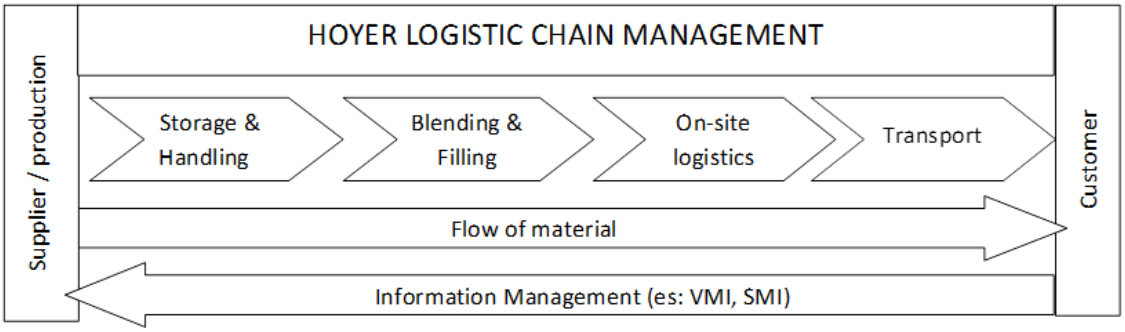
Il successo di HOYER deriva dalla sua posizione competitiva vantaggiosa che detiene grazie all'offerta di un servizio completo ai suoi clienti, con i quali ha instaurato una solida partnership e rapporto di fiducia.

HOYER offre soluzioni logistiche integrate e un servizio a tutto tondo al cliente: dalla progettazione della supply chain del cliente alla pianificazione del trasporto fino all'esecuzione del trasporto stesso completando l'offerta con i servizi accessori: *"Combiniamo tutti i servizi associati all'Intermediate Bulk Container, in linea col motto "More than just rental", che significa che non facciamo solo un servizio di noleggio e di trasporto, ma anche di pulitura, manutenzione e riparazione".* [*]

HOYER, in qualità di 3PL (Third Party Logistics) offre un ampia gamma di attività che vanno oltre al servizio di trasporto base. Insieme all'attività core (trasporto), offre una serie di attività a valore aggiunto per il cliente che sono storage & handling, blanding & filling e on-site logistics. Inoltre svolge anche il ruolo di consulente nella progettazione della logistica e delle procedure di aziende che possiedono già una logistica propria. Il tutto con una forte attenzione alla sostenibilità.

La supply chain di HOYER è la seguente:

[*] Frasi tratte dal sito aziendale di Hoyer Group



HOYER svolge un ruolo di pianificatore e di coordinatore dei flussi dei materiali a casa del cliente e fornisce un servizio completo dal ricevimento del materiale grezzo nello stabilimento, magazzinaggio del materiale che in seguito diventerà prodotto finito (storage & handling), fino al riempimento dei tank container (filling) destinati al cliente finale.

La nostra intervista si focalizzerà esclusivamente sul trasporto dal cliente produttore verso la destinazione finale.

Il contributo di Sabrina Robba offre sicuramente un punto di vista molto dettagliato sull'operato di uno dei maggiori distributori di prodotti chimici in Europa.

Adozione degli strumenti

Forza lavoro multidisciplinare

Hoyer applica in modo massiccio questo strumento ritenendolo fondamentale per il proprio business.

"Noi tendiamo ad avere autisti che siano in grado di scaricare ogni tipologia di prodotto; tuttavia, per alcune tipologie specifiche di merce, ci sono dei corsi particolari. In azienda tutte le persone coinvolte nel trasporto di merce pericolosa hanno fatto il corso ADR. Nel nostro settore l'autista non è solo colui che guida il camion ma è la persona che conosce il prodotto trasportato e quando va a ritirare o a consegnare la merce partecipa attivamente al carico o allo scarico ad esempio attaccando il tubo, facendo delle verifiche, ecc. Insomma ha un ruolo molto più ampio rispetto ai tradizionali autisti di merce non pericolosa. Ogni autista sa cosa sta trasportando e questo è molto importante soprattutto quando va a consegnare a destino; puo' capitare che i clienti non conoscano tutte le caratteristiche del prodotto

acquistato perché magari è uno dei tanti input che entra nel processo, ed hanno un approccio e una competenza diversa rispetto all'azienda chimica che lo produce." [*]

Gli impatti riguardano l'implementazione delle procedure sia per quanto riguarda gli attacchi che la fornitura.

Collaborazione tra dipendenti

Hoyer applica in modo formale anche lo strumento di collaborazione.

"Noi abbiamo quelli che vengono chiamati driver trainer, cioè autisti che hanno fatto un corso specifico denominato Behaviour Base Safety (BBS) definito dall'industria chimica a livello europeo. Tutti gli autisti faranno il training con il driver trainer però durante il lavoro quotidiano sono indipendenti." [*]

"A livello di gruppo c'è una divisione formale in team e si applica un'incentivo di gruppo per alcuni prodotti specifici (come il prodotti petroliferi e i gas criogenici) o per clienti specifici o per trasporti specifici. In realtà il concetto di team è costruito solo sulle performance (non è paragonabile al team che si può formare in ufficio). Anche se sono assegnati allo stesso mezzo gli autisti lavorano su turni diversi e quindi sono da soli quando guidano il camion." [*]

Gli impatti sono a livello operativo sia lato fornitura che, soprattutto lato attacchi.

"L'effetto è sicuramente a livello operativo, ovviamente la collaborazione ha un forte impatto sugli attacchi perché se l'autista dovesse notare qualcosa che non va deve informare chi di dovere e la collaborazione puo' generare un'efficacia maggiore." [*]

Integrità, lealtà dipendenti

Per Hoyer è molto importante disporre di operatori integri e leali, per motivare i dipendenti verso questo obiettivo si elargiscono incentivi anche di tipo economico.

"Noi abbiamo il giornalino dell'azienda dove viene riportato chi è in azienda da un certo numero di anni (5, 10, 15, fino a 40); quando si raggiungono questi è previsto un incentivo economico." [*]

Esiste un'attenzione nei riguardi del personale per garantire la sua integrità sempre in conformità con le leggi nazionali.

"Per quanto riguarda le investigazioni sul background in Svizzera è possibile ma in Italia e in altri paesi come Germania e Olanda che hanno leggi sulla privacy molto tutelanti no. In Svizzera e' utilizzato lo strumento delle referenze, e si può richiedere il

[*] Frasi estrapolate dall'intervista a Sabrina Robba, Managing Director HOYER Italia S.r.l. e di HOYER Svizera SA e responsabile della sicurezza, ambiente e qualita'del gruppo HOYER

casellario giudiziario. Per esempio in Olanda non è possibile fare dei controlli spot sul consumo dell'alcool negli autisti, mentre in Italia durante la visita medica vengono fatti test sull'alcool e la droga ma questi risultati non sono poi messi conoscenza dell'azienda, il risultato è idoneo o non idoneo." [*]

L'impatto è sull'implementazione delle procedure e sulla collusione.

Sviluppo della consapevolezza interna sulla sicurezza

In Hoyer è presente un forte impegno nel diffondere a tutti i livelli aziendali le tematiche di sicurezza come testimoniano le numerose riunioni a più livelli organizzate.

"A livello di gruppo c'è un advisory board ogni quadrimestre dove si toccano temi che riguardano la security e le performance (in cui abbiamo i late delivery, cioè quello che per voi è la sicurezza di fornitura). Dopodichè c'è un operating board in cui ci sono i responsabili delle diverse business unit (petrolog, gaslog, chimica, food e trasporti overseas); anche a questo livello vengono analizzati i temi sopracitati; a livello locale ci sono inoltre dei meeting regolari; i temi inerenti lo SHEQ, acronimo per Safety, Healty, Environmental and Quality, sono discussi come primo punto nell'agenda. A questi temi sopracitati è stata inserita la Security.

A livello operativo per gli autisti si fa invece una riunione all'anno e, ogni volta che succede qualche incidente, vengono creati dei safety flash, o organizzati brevi meeting di 5 minuti in cui vengono spiegati gli incidenti, perché sono avvenuti e come prevenirli." [*]

L'impatto è a livello operativo sul miglioramento dell'implementazione delle procedure.

Aspetti soft

Questo strumento è applicato a livello di gruppo.

"A livello di gruppo è stato pubblicato quest'anno il codice di condotta, stabilisce le linee guida per lavorare e comportarsi in maniera etica all'interno ed all'esterno dell'azienda." [*]

"Poi c'è la sustainability policy che indica le linee guida in merito alla responsabilità sociale e alla protezione dell'ambiente e la SHEQ policy in cui si pone l'attenzione alla sicurezza informativa, del trasporto e dello stoccaggio delle merci pericolose ad alto rischio seguendo le legislazioni specifiche." [*]

[*] Frasi estrapolate dall'intervista a Sabrina Robba, Managing Director HOYER Italia S.r.l e di HOYER Svizera SA e responsabile della sicurezza, ambiente e qualita'del gruppo HOYER

In Hoyer c'è un'attenzione particolare nell'implementare in modo corretto questo strumento così da avere più benefici possibili.

"Gli strumenti soft possono motivare se le cose sono gestite top down, cioè se gli operatori vedono attenzione e motivazione da parte dei line manager, anche nella management conference del Gruppo HOYER che si e' svolto ad Amburgo la settimana scorsa è stato sottolineato che quando si parla di codice di condotta i manager sono i primi a dover dare l'esempio." [*]

L'impatto principale è sull'implementazione delle procedure sia lato attacchi che fornitura, inoltre vi è un ipotetico impatto sulla collusione anche se non facilmente quantificabile.

"L'impatto è sulla motivazione e quindi sull'operatività, mentre sulla collusione è difficile valutare, io sinceramente ritengo che se una persona è intenzionata a colludere non venga scoraggiata da un codice di condotta. E' anche vero che se una persona si trova a far parte di un ambiente dove tutti hanno un'impronta etica sicuramente tenderà meno a rubare, ma non sono in grado di valutare quanto questo possa influenzarne direttamente il comportamento." [*]

Continous improvement

In Hoyer si utilizza lo strumento del Continous improvement per migliorare sia le procedure sia il modo di applicarle.

"Il principio base dell'incident investigation è quello di costituire un team di persone che analizzeranno l'incidente, coinvolgendo sempre l'autista o l'operatore in modo che ci siano le persone più a contatto con la pratica , con il job, se possibile si cerca di coinvolgere anche un driver trainer in modo che dia dei suggerimenti pratici; nel caso in cui dovesse succedere qualcosa nel luogo di scarico loro sono gli unici a conoscenza delle modalita' operative in quel luogo essendo un posto di proprietà del cliente. Le informazioni ed i suggerimenti che provengono dagli autisti vengono utilizzate per ridisegnare le working instruction a livello operativo ma anche le procedure a livello più alto." [*]

L'impatto si estende anche ai padroncini fully integrated in quanto sono trattati come se fossero autisti dipendenti

[*] Frasi estrapolate dall'intervista a Sabrina Robba, Managing Director HOYER Italia S.r.l. e di HOYER Svizera SA e responsabile della sicurezza, ambiente e qualita'del gruppo HOYER

Business continuity planning

Questo strumento non viene applicato in azienda; viste le numerose variabili in gioco è difficile creare delle soluzioni alternative prima dell'avvenimento della disruption.

"Nell'offerta al cliente ci sono diverse tratte e lui decide di acquistare quella a lui più congeniale in termini di prezzo e di delivery lead time. Non esistono però delle tratte alternative prestabilite a seguito di disruption, si decidono just in time le nuove azioni da intraprendere; comunicando sempre con il cliente per capire quelle che sono le sue esigenze." *

Segnalare incidenti e debolezze

C'è forte attenzione nel migliorare le procedure e fare in modo che queste vengano implementate in modo corretto tramite un utilizzo diffuso di questo strumento.

"Quando accadono quelli che noi chiamiamo main incident, noi abbiamo un sistema di incident investigation (che è un form da compilare con su tutte le informazioni relative e, dove vengono identificate, anche le azioni correttive e preventive per evitare che l'incidente possa accadere ancora), ma può capitare che per alcuni near misses venga considerata l'idea di fare un'incident investigation da cui poi scaturiscono una serie di azioni correttive, tra le quali una parte preponderante riguarda piani di training." *

"L'autista riporta verbalmente la situazione di pericolo o di quasi incidente ed il responsabile locale della sicurezza compila il formulario dei near miss." *

In Hoyer si cerca di incentivare l'applicazione di questo strumento.

"Nel reparto Supply Chain Solutions che fa parte della BU chimica, e' stata organizzata quest'anno una campagna di sensibilizzazione sui near misses con diversi premi per i blu collar (gli operatori). Questa iniziativa sarà replicata a livello di gruppo per l'anno prossimo. La cosa più importante è quella che quando viene segnalata un'anomalia poi venga dato un feedback a colui che ha riportato il problema." *

L'impatto di questo strumento si estende ai partner di filiera migliorando il loro stato di sicurezza.

" Ad esempio l'altro giorno mi hanno chiamato avvisandomi che al terminal c'era un tombino scoperto con potenziale rischio per l'autista di cadere nello stesso e questo è un esempio di corretto reporting da partedegli autisti." *

* Frasi estrapolate dall'intervista a Sabrina Robba, Managing Director HOYER Italia S.r.l. e di HOYER Svizera SA e responsabile della sicurezza, ambiente e qualita'del gruppo HOYER

Knowledge management

Esiste una piattaforma ad hoc per gestire la conoscenza e le esperienze passate.

"Abbiamo dei database a livello di gruppo di diverso tipo, uno viene chiamato SHEQ GROUP INFO in cui ci sono informazioni di base come la presentazione sulla sicurezza effettuata durante le riunioni e anche le performance mensili, queste informazioni sono accessibili ad ogni persona del gruppo. Un altro database si chiama SHEQ TRAINING in cui ci sono i training di tutto il gruppo, che possono essere sull'ADR, sulla guida, sui prodotti, sul risk assessment, e qua sono presenti anche tutti i near misses; poi abbiamo SHEQ MAIN INCIDENT dove sono presenti tutti i main incident corredati dal relativo incident investigation con foto, questo database è però accessibile solo a un gruppo limitato di persone per questioni di privacy. Inoltre è presente SHEQ RISK ASSESSMENT con tutte le analisi dei rischi legati all'operatività o al prodotto. Queste piattaforme sono una sorta di codificazione delle esperienze passate per metterle a disposizione di tutti." [*]

L'impatto di questo strumento è esteso a tutti i fattori causa, ad esclusione della collusione.

"Questo impatta su tutto, chiaramente deve essere utilizzato. Noi mettiamo su questo database tutte le informazioni che abbiamo; poi ogni operation manager, che ha la responsabilità del trasporto, valuta in base alla situazione locale se è interessante proporre un safety flash piuttosto che un altro, ovviamente traducendolo nella lingua locale. Ad esempio in Italia non si proporrà mai un safety flash inerente al trasporto del petrolio perché non si effettua questo tipo di trasporto." [*]

Valutazione della conformità di sicurezza

Essendo un'azienda che manipola merce pericolosa è obbligatorio possedere certificazioni che accertano determinati livelli di sicurezza, sia interni che per i fornitori.

"Noi siamo certificati secondo la norma ISO 9001, ed il nostro sistema di gestione tiene in considerazione le norme sull'ambiente, SQAS e la normativa ADR. Nelle stazioni di lavaggio (quindi fornitore inteso in termine ampio) ci sono delle stazioni di riscaldo che possono essere elettriche, ad acqua o a vapore (le più pericolose perché con una temperatura di contatto piu' elevata); durante le operazioni di riscaldo bisogna stare molto attenti con alcuni tipi di prodotti esplosivi o che tendono a polimerizzare i quali

[*] Frasi estrapolate dall'intervista a Sabrina Robba, Managing Director HOYER Italia S.r.l. e di HOYER Svizera SA e responsabile della sicurezza, ambiente e qualita'del gruppo HOYER

non possono essere riscaldati a vapore. Nel caso di merci pericolose e' obbligatorio, se non si possiedono permessi speciali, lasciare il carico su chassis; questo puo' essere un punto debole perche', in caso l'area non sia adeguatamente protetta, si potrebbe arrivare con una motrice e rubare il carico".[*]

Queste certificazioni impattano e modificano le procedure sia interne che del partner rendendole conformi agli standard di sicurezza richiesti dalla legge.

Partnership

La partnership è uno strumento applicato sia lato padroncini, sia lato operatori ferroviari.

"Gli operatori ferroviari e navali sono gestiti a livello centrale ad Amburgo, si organizzano meeting regolari, con Hupac c'è un rapporto privilegiato essendo una nostra partecipata; in generale si cerca una buona comunicazione sia con gli operatori ferroviari che con quelli navali." [*]

"La differenza fondamentale tra autisti fully integrated e quelli spot è che i fully integrated sono considerati come autisti propri: ricevono le nostre procedure, il manuale dell'autista, seguono i nostri training, c'è una procedura per la selezione, prima di effettuare dei trasporti vengono a conoscenza di quelle che sono le regole HOYER, ecc.. Invece gli spot non hanno questo tipo di integrazione, per prevenire non conformita' ed adempiere alle norme imposte dalle certificazioni ISO e SQAS si allega al contratto dei requisiti da rispettare da parte dei fornitori spot. Chiaramente la relazione è diversa." [*]

L'impatto che queste relazioni di lungo periodo hanno è sul totale dei fattori causa.

"Oltre ad adempiere meglio alle procedure, i fully integrated sono conosciuti uno ad uno e questo sicuramente impatta anche sulla collusione." [*]

" Questo rapporto consente di migliorare vicendevolmente la definizione delle procedure per quanto riguarda gli operatori ferroviari; mentre per quanto riguarda i padroncini (fully integrated) abbiamo la presunzione di ritenere che interfacciandosi con noi in questo modo migliorino loro stessi le procedure." [*]

Sviluppo della consapevolezza sulla sicurezza con i partner

Siccome ai meeting periodici partecipano anche i padroncini, lo strumento viene sicuramente applicato.

[*] Frasi estrapolate dall'intervista a Sabrina Robba, Managing Director HOYER Italia S.r.l. e di HOYER Svizera SA e responsabile della sicurezza, ambiente e qualita'del gruppo HOYER

"Inoltre facciamo dei safety check, andiamo cioè a controllare saltuariamente i padroncini su quelli che sono ad esempio tutti i dispositivi di protezione individuale, lo stato dei mezzi, delle gomme, ecc e questo da modo di avere una relazione più diretta con loro e capire il livello di sicurezza." [*]

Viene applicato anche dalle industrie chimiche nei confronti di HOYER per spiegare i pericoli connessi ai prodotti venduti; questo implica che gli impatti comprendono sia l'implementazione delle procedure, sia la definizione delle procedure.

Riduzione della differenza di cultura tra azienda e partner

Strumento applicato lato padroncini.

"Dopo il meeting annuale con gli autisti, viene organizzato un aperitivo ed un pranzo che coinvolge anche il reparto operativo; per i dipendenti c'è la cena annuale, a livello europeo una volta ogni due anni facciamo quello che si chiama european driver of the year: ogni paese che vuol partecipare selezione l'autista migliore, che può essere anche un padroncino, e in Germania facciamo una competizione basata su un test teorico, ma anche su vari test di carattere pratico, ad esempio un percorso con un camion per verificare l'abilita' di manovra, l'utilizzo di un simulatore di guida , un test sui pre-start check con un camion manomesso per verificare se l'autista identifica le non conformità, etc. In alcuni paesi come l'Inghilterra dove sono molto sensibili sui temi della sicurezza viene organizzato il safety day con dipendenti, padroncini, ecc…" [*]

L'impatto è sull'implementazione delle procedure lato attacchi e fornitura.

"Questi eventi impattano fortemente sulla motivazione degli operatori." [*]

Focus sul cliente finale

Questo strumento di filiera non è applicato.

"Nei contratti con il cliente ci possono essere delle penali legate alle prestazioni, l'incentivo potrebbe essere quello di incrementare il volume d'affari se le prestazioni sono buone. La filiera è abbastanza spezzettata". [*]

Grado di importanza degli strumenti

Gli strumenti ritenuti più importanti sono: sviluppo della consapevolezza sulla sicurezza sia interna che esterna, segnalare incidenti e debolezze, knowledge management, valutazione della conformità di sicurezza.

[*] Frasi estrapolate dall'intervista a Sabrina Robba, Managing Director HOYER Italia S.r.l. e di HOYER Svizera SA e responsabile della sicurezza, ambiente e qualita'del gruppo HOYER

Peso dei fattori causa

Per quanto riguarda la sicurezza da attacchi il fattore causa più rilevante è l'inadeguatezza delle procedure seguito da errata/mancata implementazione delle stesse, come ultima è stata citata la collusione.

"Per quella che è la mia esperienza è un problema di procedure, anche a livello europeo secondo me ci sono delle lacune, nella stesura, ma piu' spesso nell'implementazine pratica; ad esempio molto spesso il sito di stoccaggio non e' chiuso, recintato, ecc.. "[*]

Parlando di sicurezza di fornitura i fattori causa, in ordine di importanza, sono: inadeguatezza partner, errata/mancata implementazione delle politiche gestionali, mancata collaborazione/visibilità con i partner e da ultima l'inadeguatezza delle politiche gestionali.

"Il grosso problema dell'intermodale è nella ferrovia o nel navale, innanzitutto in europa non c'è un grande sviluppo del trasporto merci su ferro sia a livello di infrastruttura sia di operatori e quindi è sicuramente il collo di bottiglia del trasporto. Per definizione bisognerebbe fare pochi km dal carico al terminal e pochi dal terminal allo scarico e quindi questi tratti incidono meno, ma il routing e' spesso influenzato dalle prestazioni della parte intermodale e per alcune relazioni si privilegia il traporto su strada." [*]

Di seguito è riportata la tabella compilata durante l'intervista.

[*] Frasi estrapolate dall'intervista a Sabrina Robba, Managing Director HOYER Italia S.r.l. e di HOYER Svizera SA e responsabile della sicurezza, ambiente e qualita'del gruppo HOYER

		SICUREZZA DA ATTACCHI			SICUREZZA DI FORNITURA			
		1	2	3	2	4	3	1
	Lo strumento viene utilizzato in azienda?	Collusione	Errata/mancata implementazione delle procedure	Inadeguatezza delle procedure	Mancata collaborazione / visibilità con i partner	Inadeguatezza partner	Errata/mancata implementazione delle politiche gestionali	Inadeguatezza delle politiche gestionali
Forza lavoro multidisciplinare	**f.**		↓				↓	
Collaborazione tra dipendenti	**f.**		↓				↓	
Integrità, lealtà dei dipendenti	**f.**	↓	↓				↓	
Sviluppo della consapevolezza interna sulla sicurezza	**f.**		↓				↓	
Aspetti soft	**f.**	↓	↓				↓	
Continuous improvement	**f.**		↓	↓		↓	↓	↓
Business continuity planning	**NO**							
Segnalare incidenti e debolezze	**f.**		↓	↓	↓	↓	↓	↓
Knowledge management	**f.**		↓	↓	↓	↓	↓	↓
Valutazione della conformità di sicurezza	**f.**		↓	↓		↓	↓	↓
Partnership	**f.**	↓	↓	↓	↓	↓	↓	↓
Sviluppo della consapevolezza sulla sicurezza con i miei partner	**f.**		↓	↓		↓	↓	↓
Riduzione della differenza di cultura tra aziende e partner	**f.**		↓			↓	↓	
Focus sul cliente	**NO**							

Evidenziati in giallo gli strumenti ritenuti indispensabili per ottenere performance sicure e i principali fattori che causano una minore sicurezza da attacchi e fornitura, la scala utilizzata per i fattori causa è in ordine crescente di importanza.

La risposta "n.f." sull'utilizzo dello strumento in azienda significa che lo strumento viene utilizzato in azienda ma non in maniera standard o formale.

D.6 Hupac

Tipologia azienda: gestore terminal intermodale, operatore commerciale del trasporto ferroviario e trazionista ferroviario

Area di responsabilità diretta: cambio di modalità di traporto, servizi ferroviari e trazione ferroviaria

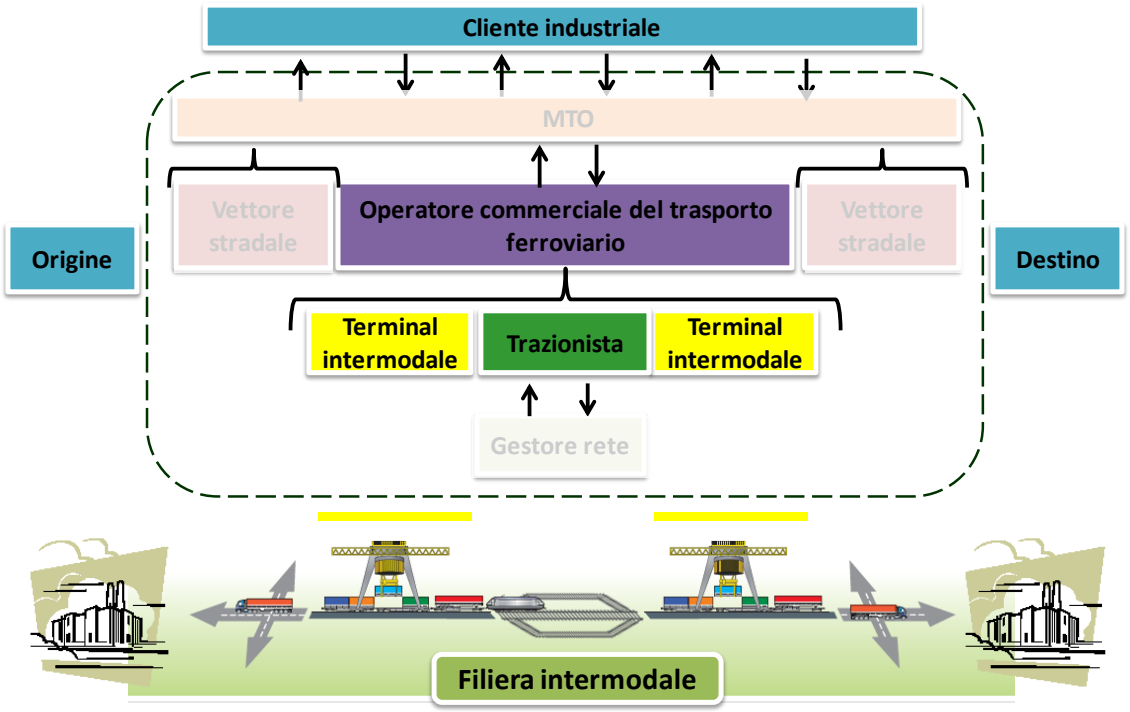
Proprietà: controllata al 72% da imprese logistiche e al 28% da imprese ferroviarie

Fatturato: 365,4 mln € (2010)

Dipendenti: 401

Interlocutore: Sergio Crespi, Direttore Generale del terminal intermodale di Busto Arsizio/Gallarate (VA)

Sede intervista: Uffici di HUPAC SpA presso il terminal intermodale di Busto Arsizio/Gallarate (VA)



Premessa

HUPAC è tra i maggiori gestori indipendenti di rete nel traffico intermodale europeo e come mission aziendale si impegna affinché "sempre più merce possa essere trasportata su rotaia anziché su strada, apportando così un importante contributo al trasferimento del traffico e alla salvaguardia dell'ambiente".

È stata fondata nel 1967 a Chiasso per iniziativa di alcuni grossi trasportatori internazionali e l'azienda svizzera di trasporto ferroviario merci (SBB).

Il business di HUPAC è composto da tre aree principale; la gestione di terminal intermodali per il cambio di modalità di trasporto, i servizi ferroviari e la trazione ferroviaria.

L'azienda si interfaccia con due tipologie di partner: da un lato con grosse imprese logistiche internazionali e dall'altro con trazionisti ferroviari.

Le grosse imprese logistiche sono i principali clienti di HUPAC che si appoggiano ad essa quando decidono di voler effettuare un trasporto intermodale delle proprie ILU, che possono essere semirimorchi, cisterne, container, casse mobili e casse telonate o furgonate. Nel tempo queste società hanno codificato la loro flotta come ferroviaria, così che sia possibile effettuare il trasporto via ferro.

HUPAC offre un servizio intermodale puro, senza stoccaggio, manipolazione e trasporto stradale e abbina a questo una specializzazione sulla parte ferroviaria, possedendo più di 5600 carri e le motrici di manovra per condurre i treni composti al fascio partenze/arrivi. È inoltre responsabilità di HUPAC l'organizzazione del trasporto via ferro con la scelta delle tracce ferroviarie da utilizzare e degli operatori principali di trazione ferroviaria, per cui ogni anno viene organizzato un bando di concorso in base al rapporto qualità/prezzo.

I fornitori di HUPAC sono invece i trazionisti ferroviari, ai quali l'azienda cede i treni completi e verificati pronti per essere trasportati su rotaia.

Un'altra parte del business è composto dai servizi ferroviari, che HUPAC effettua per i propri fornitori, e che comprendono la composizione/formazione del treno, la verifica e la prova freno da effettuare prima della partenza, e la movimentazione del treno completo fino al fascio di arrivi/partenze.

In realtà HUPAC dal 2003 è anche un operatore ferroviario e, possedendo le locomotive, avrebbe la possibilità di svolgere in prima persona il trasporto su ferro;

questo si verifica però raramente, e solamente quando c'è necessità di sopperire ad alcune lacune di disponibilità degli operatori ferroviari esterni.

L'azienda non si interfaccia mai con il cliente industriale (finale) della filiera intermodale.

L'azienda gestisce in prima persona 10 terminal intermodali, e collabora con più di 60 terminal in tutta Europa. Negli ultimi anni, inoltre, la politica aziendale prevede un continuo sviluppo del parco terminalistico, che ha visto la recente realizzazione di due nuovi terminal ad Anversa.

HUPAC gestisce con la rete Shuttle Net (rete per trasporti intermodali di alta qualità punto a punto) i traffici in tutta Europa, dalla Spagna alla Russia con asse principale nord Italia-Germania/Benelux.

In aggiunta con l'aumento di competitività del trasporto su rotaia rispetto a quello su nave, l'azienda ha iniziato a gestire i primi treni verso l'estremo oriente con prospettive interessanti di sviluppo.

La nostra intervista si è concentrata sull'operato del terminal di Busto Arsizio/Gallarate, che dal 2005 (dopo i lavori di ampliamento sulla parte di Gallarate) è il terminal più importante d'Europa per grandezza e volume movimentato.

Il terminal possiede 13 binari serviti da gru per il trasbordo, 5 binari di servizio, 5 binari di presa/consegna e 12 gru a portale. Ha la capacità teorica di formare 34 coppie di treni al giorno (oggi ne realizza circa 25 al giorno) che collegano il terminal a sud Italia, Germania, Svizzera, Belgio, Danimarca e Svezia. Ha un'estensione di 242800 mq e movimenta giornalmente 1750 ILU corrispondenti a 35000 tonnellate. È aperto 7 giorni alla settimana 24h non stop e impiega più di 230 dipendenti.

Al giorno d'oggi, venendo trasportata qualsiasi tipologia di merce su ferro, l'esigenza di avere un terminal sicuro è basilare per HUPAC. Infatti anche se è vero che l'azienda non offre un servizio di stoccaggio dei contenitori, in ogni caso questi possono subire una sosta tecnica nel terminal fino ad un massimo di 36 ore, nelle quali deve esserne garantita l'integrità.

La sicurezza da attacchi è quindi basilare per l'azienda che negli anni si è dotata di un sistema d'allarme perimetrale anti-intrusione, di un sistema di vigilanza e di telecamere a circuito chiuso, oltre alle classiche barriere fisiche da difesa.

Attualmente il terminal di Busto Arsizio/Gallarate è riconosciuto come uno dei più sicuri d'Europa e questo è anche il suo principale biglietto da visita verso i propri clienti.

Il contributo di Sergio Crespi offre un punto di vista a 360 gradi sull'operato del principale terminal intermodale d'Europa.

Adozione degli strumenti

Forza lavoro multidisciplinare

HUPAC si impegna nel formare una forza lavoro multidisciplinare.

"Soprattutto per garantire un servizio di qualità alla clientela è importante che gli operatori abbiano una competenza più ampia rispetto a quella che è la loro mansione. Facciamo dei corsi semestrali ai quali gli operatori devono partecipare per formarli su varie tipologie di problematiche, quindi possiamo dire senz'altro che la nostra forza lavoro è multidisciplinare".[*]

Per quanto riguarda gli impatti della forza lavoro multidisciplinare sono stati individuati nell'errata/mancata implementazione delle procedure sia lato attacchi che fornitura.

"Sicuramente abbassa la probabilità che si verifichino delle problematiche. Noi abbiamo delle procedure importanti soprattutto a livello di controllo in uscita e il rischio di un errore umano c'è sempre, anche se gli strumenti elettronici ci danno una mano in questo.

Aiuta anche per la sicurezza di fornitura perché dovete fare conto che per preparare un treno devo chiuderlo, manovrarlo, controllarlo e verificarlo in circa un'ora. Se qualsiasi di queste operazioni non viene fatta al meglio vuol dire fare ritardo sulla consegna e a volte perdere la traccia e magari consegnare il treno il giorno dopo con conseguenze enormi". [*]

Collaborazione tra dipendenti

La collaborazione tra dipendenti è ritenuta un elemento indispensabile a tutti i livelli.

"Per fare la nostra movimentazione abbiamo gli aiuto gruisti, i gruisti, i manovratori, il macchinista, il formatore, il verificatore, il coordinatore di piazzale, il coordinatore di settore e il macchinista manovratore che porta fuori il treno. È evidente che tutti questi devono sentirsi facenti parte di un unico team affinchè ognuno faccia la cosa giusta al momento giusto e subito.

[*] Frasi estrapolate dell'intervista a Sergio Crespi, Direttore Generale del terminal HUPAC di Busto Arsizio/Gallarate

Abbiamo un'ingegneria turnistica articolatissima per cui il team viene creato tenendo conto delle caratteristiche delle persone; per esempio i gruisti vengono messi nella postazione dove si sa che lavorano meglio, e il sistema fa questo calcolo particolare. Quello del gruppo è uno degli aspetti che noi enfatizziamo maggiormente".[*]

Per quanto riguarda un'incentivazione economica da attribuire al team, attualmente non viene praticata.

"Abbiamo fatto esperimenti di vario tipo ma fondamentalmente la politica delle incentivazioni è sulla professionalità, e quindi più sei bravo e ottieni una qualifica importante e più ti retribuisco. Non è mai stato fatto a livello di team, anche perché il team è fisso per una settimana ma poi con la politica di rotazione cambia sempre un po' per le assenze, malattie, ferie infortuni, e un po' perché ritengo controproducente tenere sempre lo stesso team per tutto l'anno.

È quindi per scelta che non abbiamo un'incentivazione di questo tipo". [*]

L'impatto di questa politica è ritenuta non rilevante per diminuire gli episodi di collusione, ma fondamentale per ottenere un risultato operativo di qualità, con conseguenze sia lato attacchi che fornitura.

Integrità, lealtà dei dipendenti

HUPAC ritiene che avere un personale fidelizzato, creare un ottimo clima aziendale e far sentire i dipendenti al centro dell'azienda sia importante per evitare episodi di collusione.

Non esiste una politica formale per premiare l'integrità e la lealtà dei dipendenti, ma si è cercato di raggiungere l'obiettivo con l'istituzione di momenti d'incontro periodici durante l'anno tra manager e operai, e incontri tra il personale di uno stesso settore.

Sviluppo della consapevolezza interna sulla sicurezza

L'azienda, come detto in precedenza, organizza delle riunioni durante l'anno che servono per discutere delle procedure e delle problematiche di sicurezza; il colloquio individuale tra i dipendenti e il Direttore Generale del terminal, è un altro momento di analisi e discussione.

Nelle riunioni sono spesso messe in atto delle campagne di comunicazione relative a specifiche tematiche di sicurezza che impattano sulla qualità del lavoro, intesa come errata/mancata implementazione delle procedure sia lato attacchi che fornitura.

[*] Frasi estrapolate dell'intervista a Sergio Crespi, Direttore Generale del terminal HUPAC di Busto Arsizio/Gallarate

Non esiste una figura o funzione preposta per la sicurezza; esistono contratti esterni con Istituti di Vigilanza prevalentemente per questioni di Safety.

Aspetti soft

L'azienda è dotata sia di un regolamento aziendale che di un codice etico.

"Sono una serie di strumenti che servono a fidelizzare i nostri dipendenti e coinvolgerli nel contesto aziendale".[*]

Oltre a questi strumenti più formalizzati, vengono ritenuti importanti per la creazione di un buon clima aziendale tutti quelle accorgimenti che servono per far identificare i dipendenti con l'azienda.

"Cerco di stare molto attento a quegli aspetti che riguardano il simbolismo, il mito e questo tipo di cose, e sono aspetti che spesso sono ripresi nelle nostre riunioni. Cerchiamo di portare avanti determinati linguaggi, motti o esempi di comportamenti che divulghiamo anche con l'aiuto di slide o filmati che mirano a creare dell'identificazione nei confronti dell'azienda da parte del lavoratore".[*]

Gli impatti di questa politica sono ritenuti molteplici. Sicuramente da un lato l'identificazione nell'azienda ha un effetto positivo nell'evitare episodi di comportamenti collusivi da parte dei dipendenti.

"Sicuramente hanno un impatto sulla collusione, d'altronde più ti senti parte di una famiglia e più ti comporti bene". [*]

Un altro effetto è dell'instaurazione del buon clima aziendale è sulla motivazione dei dipendenti che si riflette nella errata/mancata implementazione delle procedure sia lato attacchi che fornitura.

L'ultimo effetto è infine stato individuato sull'inadeguatezza delle procedure; infatti se i dipendenti si sentono partecipi e maggiormente coinvolti nella vita aziendale sono senza dubbio meno restii e più motivati nel dare consigli e suggerimenti per migliorare le politiche gestionali.

Continous improvement

È una politica aziendale quella di cercare di far sentire tutti i dipendenti al centro dell'azienda, anche dando loro la possibilità di proporre nuovi metodi e procedure.

[*] Frasi estrapolate dell'intervista a Sergio Crespi, Direttore Generale del terminal HUPAC di Busto Arsizio/Gallarate

"Abbiamo creato dei momenti importanti per i dipendenti. Abbiamo dei colloqui individuali, circa due o tre volte l'anno, in cui in fase di distribuzione degli stipendi ciascun dipendente parla col sottoscritto.

Abbiamo istituito altri incontri periodici a livello di reparti e con il responsabile della sicurezza del terminal e abbiamo creato una cassetta delle idee, nella quale tutti possono lasciare dei suggerimenti senza dover parlare con me direttamente".[*]

Si può quindi dire che il processo di miglioramento continuo in azienda è presente e formalizzato, e nel corso degli anni ha portato ad ottimi risultati.

"Devo dire che molte delle idee suggerite sono state applicate, magari non con i tempi richiesti dai dipendenti che non possono avere anche una visione strategica, ma comunque il feedback è stato molto importante".[*]

L'azienda ha deciso di non legare questo processo ad un incentivo di tipo economico per non rischiare di creare tensioni e invidie tra gli stessi dipendenti.

"Preferisco valutare globalmente l'operato di una persona, e nella valutazione rientra sicuramente anche quest'aspetto che però non viene ufficializzato. Possiamo dire che quindi non abbiamo un sistema di incentivazione formale ma che prendiamo in considerazione a 360 gradi l'operato di una persona".[*]

L'impatto del continous improvement è stato ritenuto impattante sia per il miglioramento delle procedure esistenti che per il miglioramento delle politiche gestionali sia lato attacchi che fornitura.

Business continuity planning

In caso di situazioni impreviste, e con riferimento al trasporto ferroviario, esistono dei piani d'azione alternativi da seguire.

"Abbiamo delle unità di crisi soprattutto a livello di manager degli assi ferroviari a Chiasso che valutano tutte queste situazioni. Un esempio eclatante recente è stata la chiusura di una direttrice del tunnel del Sempione per un incendio; abbiamo dovuto sfruttare una linea di trasporto diversa che passa da Chiasso piuttosto che da Luino, che è la nostra linea classica. È quindi evidente che noi ci teniamo sempre delle soluzioni alternative per ovviare a queste situazioni". [*]

[*] Frasi estrapolate dell'intervista a Sergio Crespi, Direttore Generale del terminal HUPAC di Busto Arsizio/Gallarate

Inoltre HUPAC potendo anche svolgere in prima persona il trasporto ferroviario può sopportare tutte quelle situazioni impreviste che riguardano l'indisponibilità dei trazionisti ferroviari come gli scioperi.

L'impatto di questi strumenti è stato identificato a livello dei processi operativi con riferimento alla sicurezza di fornitura.

Segnalare incidenti e debolezze

Per quanto riguarda la segnalazione di incidenti e debolezze sono presenti dei meccanismi formali che riguardano l'intera tratta ferroviaria.

"Per quanto riguarda la ferrovia è tutto regolamentato. Abbiamo un ufficio di affari generali e legali che curano al 90% solo queste situazioni ed in più il regolamento ferroviario sia italiano che europeo disciplina le responsabilità dei singoli vettori. In generale una volta consegnato il treno completo all'operatore ferroviario, questo viene verificato, e tutte le problematiche che emergono durante la tratta successiva via ferro sono responsabilità del trazionista".[*]

Per quanto riguarda il focus sui near messes è presente un sistema integrato di valutazione della qualità (SGS) che si adatta anche a queste situazioni.

L'impatto di questa politica sulle segnalazioni è ritenuta importante oltre che per l'aspetto legale/assicurativo, anche per capire dove migliorare le procedure esistenti ed eventualmente dove cambiare delle politiche gestionali, sia lato attacchi che fornitura.

Knowledge management

HUPAC non utilizza un software per la gestione della conoscenza.

"Non abbiamo uno strumento di questo tipo. Facciamo formazione e istruzione sul campo e il meccanismo del team ci aiuta nella diffusione della conoscenza".[*]

Valutazione della conformità di sicurezza

HUPAC è certificata ISO 9001 per quanto riguarda il sistema di gestione della qualità e ISO 14001 per quanto riguarda il sistema di gestione ambientale.

"Per noi è importante che tutti i nostri partner siano certificati. Essendo noi certificati ISO 9001 e ISO 14001 avere clienti e fornitori certificati ci garantisce qualità a 360 gradi".[*]

Le certificazioni hanno secondo il nostro interlocutore un duplice impatto: da un lato garantiscono la possibilità di poter costruire un processo fluido di filiera, nel quale

[*] Frasi estrapolate dell'intervista a Sergio Crespi, Direttore Generale del terminal HUPAC di Busto Arsizio/Gallarate

HUPAC si trova ad avere a che fare con attori sulla stessa lunghezza d'onda. Dall'altro lato la certificazione può anche essere vista con un significato etico, garantendo sulla professionalità dei partner di filiera.

Partnership

HUPAC privilegia relazioni di lungo periodo a tutti i livelli.

"L'organizzazione di un servizio ferroviario è talmente complesso che se tutti gli anni dovessi rimettere in discussione tutti i nostri partner sarebbe molto problematico. La fidelizzazione può essere intesa anche in questo senso, con riferimento ai partner di filiera". [*]

Lo sviluppo di partnership è ritenuta un elemento imprescindibile con impatti positivi su tutti i fattori causa relativi alla sicurezza da attacchi e fornitura.

Più degli altri è stato ritenuto importante l'aspetto che riguarda l'integrazione e la trasparenza che HUPAC instaura con i propri partner.

"Abbiamo un sistema che si chiama Goal (Global Oriented Application for Logistic) attraverso il quale tutti i nostri partner possono avere in tempo reale informazioni riguardanti le loro unità di carico. Il sistema mostra informazioni in aggiornamento costante rispetto a dove si trovano, quando verranno ritirate, quando verranno consegnate, se ci sono stati dei problemi in linea e così via. Penso che la trasparenza sia la nostra maggiore forza". [*]

Sviluppo della consapevolezza sulla sicurezza con i partner

HUPAC si pone come promotore delle iniziative di formazione continua in relazione alla sicurezza all'interno della filiera, e molto spesso si assume anche il compito di educare i partner per ottenere prestazioni di filiera migliori.

Per quanto riguarda i contratti con i propri partner, vengono esplicitati i requisiti di sicurezza lato fornitura, quindi il livello di servizio minimo che HUPAC dovrà rispettare, mentre non sono presenti esplicite clausole sui furti, per i quali l'azienda deve rispondere solo in caso avvengano nel terminal.

Queste politiche garantiscono un impatto sull'errata/mancata implementazione delle procedure sia lato attacchi che fornitura.

[*] Frasi estrapolate dell'intervista a Sergio Crespi, Direttore Generale del terminal HUPAC di Busto Arsizio/Gallarate

Riduzione della differenza di cultura tra azienda e partner

HUPAC è anche molto attiva nell'organizzazione di iniziative di incontro e socializzazione informale con i partner di filiera.

"Tutti gli anni facciamo delle customer convention parlando della sicurezza a 360 gradi, oltre che della parte commerciale, piuttosto che del servizio alla clientela, della qualità, della puntualità dei treni eccetera. Queste iniziative ci servono per migliorare la collaborazione e l'integrazione con i partner e la loro fidelizzazione. Sono iniziative rivolte sia ai nostri clienti che ai nostri fornitori che servono per migliorare la qualità della partnership".[*]

Gli impatti di queste iniziative sono stati individuati oltre che sulla mancata collaborazione e visibilità, anche sull'inadeguatezza del partner e sull'inadeguatezza delle politiche gestionali sia lato attacchi che fornitura.

Focus sul cliente finale

Per quanto riguarda HUPAC non esiste una reale ottica di filiera ed ogni attore si concentra esclusivamente sulla parte di propria responsabilità.

"Noi come HUPAC non sappiamo neanche dove sarà la consegna finale dei treni che componiamo. Non fa parte del nostro business e non è di nostro interesse".[*]

Grado di importanza degli strumenti

Tra gli strumenti analizzati quelli ritenuti indispensabili per ottenere performance sicure sono stati individuati nella collaborazione tra dipendenti, nell'integrità/lealtà dei dipendenti, nello sviluppo della consapevolezza interna sulla sicurezza e nella segnalazione di incidenti e debolezze.

"La segnalazione di incidenti e debolezze è fondamentale perché è sulla base dell'esperienza e dei punti di debolezza che si riesce a migliorare un'organizzazione. Io poi credo molto negli strumenti interni perché penso che creare un ottimo clima e una forte cultura aziendale sia determinante a tutti i livelli".[*]

[*] Frasi estrapolate dell'intervista a Sergio Crespi, Direttore Generale del terminal HUPAC di Busto Arsizio/Gallarate

Peso dei fattori causa

Per quanto riguarda la sicurezza da attacchi, la mancanza di sicurezza dipende in ordine d'importanza dall'errata/mancata implementazione delle procedure operative, dall'inadeguatezza delle politiche gestionale e per ultimo dalla collusione.
Per quanto riguarda la sicurezza di fornitura l'inadeguatezza del partner è stata individuata come la causa principale dei ritardi provocati al cliente finale. Come secondo fattore causa è stata individuata la mancanza di collaborazione e visibilità con i partner e successivamente l'inadeguatezza delle politiche gestionali e l'errata o mancata implementazione delle procedure operative.

Di seguito è riportata la tabella compilata durante l'intervista.

		SICUREZZA DA ATTACCHI			SICUREZZA DI FORNITURA			
		1	3	2	3	4	2	2
	Lo strumento viene utilizzato in azienda?	Collusione	Errata/mancata implementazione delle procedure	Inadeguatezza delle procedure	Mancata collaborazione / visibilità con i partner	Inadeguatezza partner	Errata/mancata implementazione delle politiche gestionali	Inadeguatezza delle politiche gestionali
Forza lavoro multidisciplinare	**f.**		↓				↓	
Collaborazione tra dipendenti	**f.**		↓				↓	
Integrità, lealtà dei dipendenti	**n.f.**	↓						
Sviluppo della consapevolezza interna sulla sicurezza	**f.**		↓				↓	
Aspetti soft	**f.**	↓	↓	↓			↓	↓
Continuous improvement	**f.**		↓	↓			↓	↓
Business continuity planning	**f.**						↓	
Segnalare incidenti e debolezze	**f.**		↓	↓			↓	↓
Knowledge management	**NO**							
Valutazione della conformità di sicurezza	**f.**	↓		↓				↓
Partnership	**f.**	↓	↓	↓	↓	↓	↓	↓
Sviluppo della consapevolezza sulla sicurezza con i miei partner	**f.**		↓				↓	
Riduzione della differenza di cultura tra aziende e partner	**f.**			↓	↓	↓		↓
Focus sul cliente	**NO**							

Evidenziati in giallo gli strumenti ritenuti indispensabili per ottenere performance sicure e i principali fattori che causano una minore sicurezza da attacchi e fornitura, la scala utilizzata per i fattori causa è in ordine crescente di importanza.

La risposta "n.f." sull'utilizzo dello strumento in azienda significa che lo strumento viene utilizzato in azienda ma non in maniera standard o formale.

D.7 Interporto Rivalta Scrivia

Tipologia azienda: terminal intermodale e MTO puro

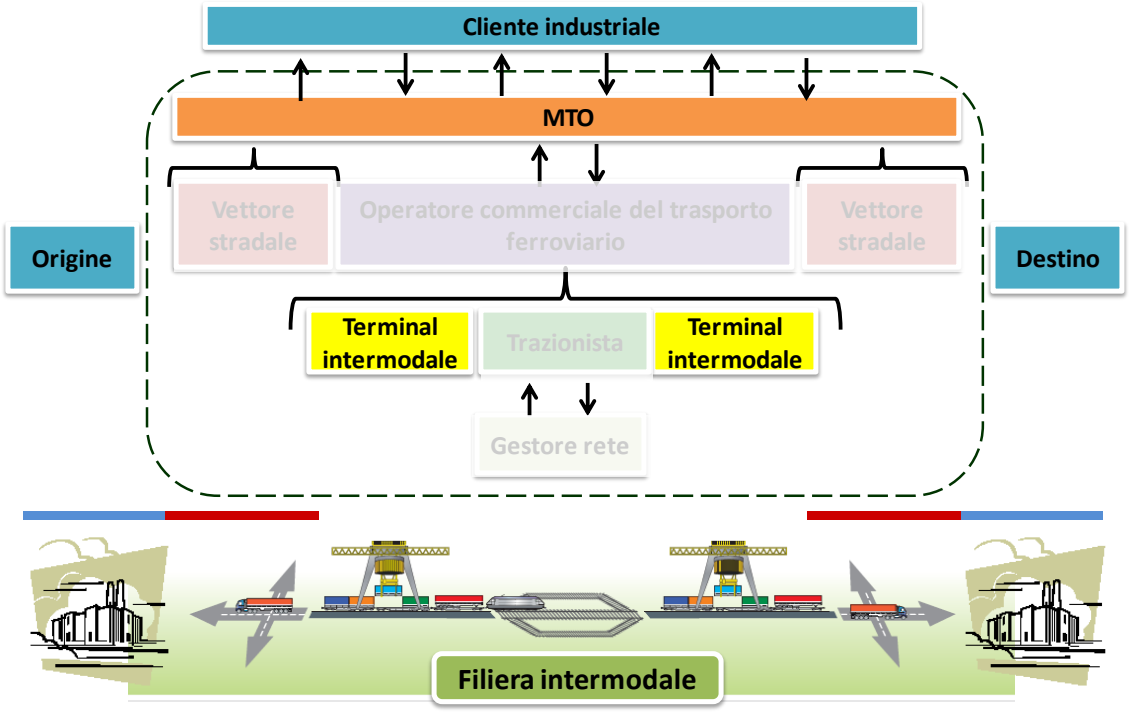
Area di responsabilità diretta: pianificazione del trasporto, gestione rapporto con il cliente, cambio di modalità di trasporto, stoccaggio.

Fatturato: 52 mln €

Dipendenti: 600 (tra cui 500 tramite cooperativa)

Interlocutore: Gian Luca Fossati, Sales & Marketing

Sede intervista: Uffici di Interporto Rivalta Scrivia S.p.A. presso Rivalta Scrivia (AL)



Premessa

L'interporto di Rivalta Scrivia, situato al centro del triangolo industriale Milano-Genova-Torino, opera nel segmento delle infrastrutture logistiche e dell'intermodalità e rappresenta la più grande infrastruttura logistica del Paese a conduzione diretta. La società è controllata dal gruppo Fagioli, leader nel comparto dell'ingegneria applicata ai trasporti e dei sollevamenti eccezionali, ed è soggetta all'attività di direzione e coordinamento di Fagioli Finance S.p.A., holding del gruppo.

Il gruppo Interporto Rivalta Scrivia è composto da due aziende: la società Interporto Rivalta Scrivia si occupa direttamente di tutte quelle che sono le operazioni logistiche, dalla ricezione delle merci, alla movimentazione e stoccaggio, fino alla semi lavorazione e all'inoltro al cliente finale, oltre che alla gestione del rapporto con i clienti industriali. La seconda società del gruppo nata nel 2006 è Rivalta Terminal Europa (in partnership con il gruppo Gavio, enti e istituzioni locali), un operatore intermodale che si occupa di tutte le operazioni relative al cambio di modalità di trasporto strada/ferrovia.

Dagli anni Sessanta, l'interporto gestisce i flussi marittimi e terrestri di differenti tipologie di merci nazionali ed estere, governandone l'intero ciclo: ricevimento (via treno o via gomma), stoccaggio presso i propri magazzini, eventuale lavorazione, smistamento, distribuzione finale.

Oggi, l'interporto di Rivalta Scrivia, è un polo logistico multifunzionale unico per la sua capacità di proporre soluzioni operative integrate, per le dimensioni delle aree e dei depositi, per la completezza dei servizi offerti e, infine, per la capacità di gestire attività di trasporto distribuzione finale delle merci, anche con soluzioni di trasporto combinato.

L'offerta di servizi dell'interporto è completata dai servizi tipici dei terminal portuali, grazie alla presenza interna di una sezione della Dogana di Genova e di un Terminal per tutte le attività di trasbordo, deposito, movimentazione e riparazione di container, rappresentando quindi una banchina remota del porto di Genova.

Oltre a essere collegato al porto di Genova, l'Interporto è direttamente collegato attraverso il sistema ferroviario e stradale con l'area portuale dell'alto Tirreno, le regioni settentrionali italiane e le nazioni confinanti dell'Europa del sud.

L'azienda per quanto riguarda la parte intermodale offre due tipi di servizi: il primo è quello dell'organizzazione e gestione di due coppie di treni shuttle al giorno dal porto di Genova all'interporto. L'altro è invece il servizio intermodale classico che collega

l'interporto di Rivalta ai clienti industriali, mediante l'organizzazione del trasporto via ferro con treni shuttle e via strada, con direttrici principali prevalentemente nel centro Italia. Per le attività di trasporto fisico delle merci, l'azienda si avvale di una rete di padroncini e un operatore commerciale del trasporto ferroviario per quanto riguarda la tratta via ferro. Quest'ultimo servizio negli ultimi anni sta incrementando sempre più in richieste e volumi, soprattutto grazie al contributo di grandi multinazionali della GDO che ripongono sempre più attenzione al trasporto ecocompatibile delle merci. Nei prossimi anni sono previsti delle direttrici verso il Triveneto, la Campania e la Sicilia.
Il gruppo Rivalta attualmente non possiede casse mobili e carri ferroviari, ma li noleggia a Trenitalia.
L'infrastruttura su cui opera l'interporto si estende su un'area di circa 1,4 milioni di m^2, di cui circa 350 di superficie coperta e circa 300 di piazzali per l'attività di terminal ferroviario e intermodale. Tramite Rivalta Terminal Europa è stata inoltre avviata la realizzazione di un nuovo terminal ferroviario su una superficie di ulteriori 800.000 m^2 adiacenti all'interporto di Rivalta Scrivia.
La superficie è dotata di un sistema di allarme e sorveglianza, essendo anche area doganale e necessitando di un controllo 24 ore su 24.
L'intero interporto impiega una forza lavoro pari a 650 persone, suddivisi tra un centinaio di dipendenti e circa 500 di cooperativa, e garantisce una capacità di carico/scarico di più di 1000 truck al giorno.
Rivalta si propone come un interlocutore privilegiato per la gestione dei processi di razionalizzazione logistica con un forte orientamento al cliente, oltre ad essere un moderno operatore logistico dotato di infrastrutture all'avanguardia, di mezzi propri idonei a soddisfare le esigenze distributive dei propri clienti, di tecnologie informatiche specializzate e un management affidabile e qualificato.
Rivalta è dotata di un proprio WMS e di un reparto IT interno. In questo modo la struttura è in grado di fornire servizi personalizzati e di mantenere costantemente aggiornati ed efficienti i sistemi che dialogano con le maggiori ditte di autotrasporto per garantire la massima precisione e rapidità nella consegna dei prodotti spediti.
Il contributo di Gian Luca Fossati offre una visione del lavoro di un polo logistico e intermodale unico nel panorama italiano.

Adozione degli strumenti

Forza lavoro multidisciplinare

L'azienda si impegna nel formare una forza lavoro multidisciplianare.

"Ovviamente ognuno ha la sua mansione, ma in azienda c'è sicuramente questo discorso di formare gli operatori non solo sul loro lavoro specifico. Questo anche perché la nostra è un'azienda molto complessa che deve fare diverse attività, e avere una visione d'insieme aiuta quando c'è un problema da affrontare".[*]

L'impatto è stato individuato a livello operativo sia per quanto riguarda gli attacchi che la fornitura.

Collaborazione tra dipendenti

L'attenzione al lavoro in team è costantemente presente in Interporto Rivalta.

"In azienda abbiamo due amministratori delegati. Uno si occupa di amministrazione, finanza e aspetti commerciali, mentre l'altro si occupa esclusivamente della formazione e gestione delle risorse umane, e il riferimento alla squadra è sempre presente. C'è un controllo costante anche perché gestire 650 addetti non è un compito facile, e nel confronto quotidiano con le direzioni operative viene deciso se spostare o meno una persona in un'altra unità operativa, se questa non rende come desiderato o potrebbe rendere di più in un altro contesto".[*]

L'impatto di questa attenzione alla gestione delle risorse umane e dei team di lavoro è stato individuato sullo svolgimento del lavoro quotidiano con riflessi sia sulla sicurezza da attacchi che di fornitura.

In azienda esiste anche una politica per incentivare formalmente il buon lavoro di squadra, applicato mediante incentivi economici a fine anno.

"Esiste una politica di premi di contribuzione nel momento in cui si raggiungono determinati obiettivi, che possono essere individuali o di squadra". [*]

Un altro beneficio del team è stato individuato sulla collusione.

"Un team di lavoro coeso potrebbe individuare più facilmente eventuali mele marce che sono presenti nell'organizzazione. La relazione tra collaborazione e collusione non è diretta e immediata, ma sicuramente il team aiuta anche in questo È ovvio che questo processo è più facile se è il singolo che agisce in maniera isolata, mentre se sono coinvolte più persone, magari anche d'accordo con il trasportatore, questa diventa una

[*] Frasi estrapolate dall'intervista a Gian Luca Fossati, ufficio Sales&Marketing di Interporto Rivalta Scrivia

*vera e propria organizzazione criminale e quindi diventa più difficile e lungo intervenire".**

Integrità, lealtà dei dipendenti

Per i dipendenti d'azienda, e anche per quelli di cooperativa, esiste una politica per premiare l'integrità e la fedeltà dei dipendenti che si manifesta con riconoscimenti sia economici che a livello di responsabilità operative.

Legato agli aspetti di integrità e lealtà dei dipendenti, una problematica che deve gestire l'azienda è il rapporto con i lavoratori di cooperativa che lavorano nei magazzini di Interporto Rivalta.

*"Da questo punto di vista Rivalta è unica nel suo genere perché abbiamo deciso di mettere una persona all'interno della cooperativa che si occupa di reclutamento e formazione del personale. Quindi pur essendo esterni gli operatori sono assolutamente formati e gestiti come i nostri e per noi questo è fondamentale per poter fare un servizio di qualità. C'è dire che anche dal punto di vista retributivo le cooperative da noi stanno molto bene, proprio perché vogliamo che sia incentivati a lavorare con attenzione e qualità".**

L'impatto delle politiche di integrità e lealtà dei dipendenti sono state individuate sulla motivazione degli stessi, con impatto a livello operativo sull'errata/mancata implementazione delle procedure sia lato attacchi che fornitura.

Sviluppo della consapevolezza interna sulla sicurezza

Interporto Rivalta oltre ai normali incontri per la sicurezza sul lavoro, svolge corsi di formazione periodici con focus sulla security.

*"Abbiamo dei corsi sulla sicurezza che tutti siamo chiamati a svolgere. Nei corsi si parla soprattutto di procedure di sicurezza, e si spiega sia come risolvere dei problemi pratici che della gerarchia che si deve seguire quando si verificano determinate problematiche. In più si fa un punto della situazione su quelle che sono le lacune del processo".**

L'impatto dei corsi si riscontra direttamente nell'operatività quotidiana mediante una maggiore consapevolezza nell'implementazione delle procedure.

* Frasi estrapolate dall'intervista a Gian Luca Fossati, ufficio Sales&Marketing di Interporto Rivalta Scrivia

Aspetti soft

L'azienda è dotata di un codice etico e di un organismo di vigilanza delle attività e delle procedure aziendali.

"Può essere vista anche come un'azione di marketing, ma da noi è principalmente uno strumento di lavoro. E' solo negli ultimi anni infatti, visto anche che è stato costruito un sito aziendale nuovo, che il codice viene divulgato verso l'esterno, mentre nel passato è sempre stato uno strumento esclusivamente interno. Regola i comportamenti che si devono tenere in azienda ed è applicato a tutti i livelli. Devo dire che il nostro è un codice etico reale, nel senso che chi non lo rispetta va incontro a sanzioni importanti. La direzione è molto attenta su questo aspetto". *

Gli impatti degli aspetti soft sono stati individuati sul fattore causa collusione e anche sulla motivazione dei dipendenti, con effetto sull'errata/mancata implementazione delle procedure per quanto riguarda la sicurezza da attacchi.

Continous improvement

Interporto Rivalta non ha una politica formale per incentivare le idee dal basso.

Negli incontri periodici sulla security però, oltre alla parte di formazione c'è anche spazio per la discussione e per accogliere dei suggerimenti da parte degli operatori.

"Capita spesso che il feedback degli operatori sia utile per migliorare delle procedure ad alto livello. A questo proposito non abbiamo una procedura formale per raccogliere i suggerimenti, ma sfruttiamo i momenti di incontro per discutere ed accogliere le idee migliori". *

L'impatto è stato individuato sia lato attacchi che fornitura sull'inadeguatezza delle procedure.

Business continuity planning

Interporto Rivalta ha definito per tutti i suoi maggiori clienti dei piani d'azione alternativi in caso si verifichino dei problemi sulla linea base del trasporto.

"Ovviamente ci sono i casi nei quali bisogna gestire l'eccezione, ma in generale c'è sempre una procedura da seguire in caso si verifichi un problema. Parlando di intermodale poi, sono anche i nostri clienti che richiedono un trasporto di backup in caso si verifichi un problema sulla tratta principale. La merce deve sempre avere una

* Frasi estrapolate dall'intervista a Gian Luca Fossati, ufficio Sales&Marketing di Interporto Rivalta Scrivia

strategia alternativa a quella classica di trasporto, che potrebbe voler dire per esempio fare il traposto tutto su gomma, perché i clienti vogliono sempre la massima tutela". *

L'impatto di questa politica è stata individuata sull'inadeguatezza delle procedure principalmente lato fornitura ma anche lato attacchi.

Segnalare incidenti e debolezze

In azienda non esiste un metodo formale per la segnalazione di incidenti e debolezze. Esiste una gerarchia conosciuta da tutto il personale, per cui l'operatore che rileva un incidente reale o potenziale deve comunicarlo al suo caporeparto, il quale si rivolgerà alla persona di interporto che ne è responsabile, il quale lo comunicherà al proprio caporeparto che lo riporterà al direttore operativo.

"E' sicuramente indispensabile che vi sia una comunicazione dal basso verso l'alto. Al momento non abbiamo uno strumento formale per fare questo, ma lo facciamo in modo informale seguendo la gerarchia. Lo strumento è sicuramente indispensabile perché è chi fa il lavoro che si accorge per primo se ci sono dei vuoti o delle cose da migliorare". *

L'impatto diretto della segnalazione è stato individuato sull'inadeguatezza delle procedure sia lato attacchi che fornitura, e indirettamente riguarda anche l'errata/mancata implementazione delle procedure.

Knowledge management

L'azienda non ha un sistema formale per la diffusione e gestione della conoscenza e dell'esperienza dei singoli dipendenti.

"Le conoscenze in ogni caso devono essere condivise, e questo avviene nella quotidianità del lavoro mediante collaborazione e lavoro in team". *

L'impatto di questo strumento è stato rilevato a livello operativo sia lato attacchi che fornitura, mentre per quanto riguarda la collusione l'effetto è stato ritenuto ambiguo.

"Teoricamente la condivisione di informazioni e conoscenza potrebbe aiutare anche per individuare episodi di collusione. In realtà potrebbe avere anche l'effetto opposto perché facendo circolare le informazioni a tutti i livelli i lavoratori potrebbero imparare sia come fare a fare le cose per bene che come fare per farle male". *

* Frasi estrapolate dall'intervista a Gian Luca Fossati, ufficio Sales&Marketing di Interporto Rivalta Scrivia

Valutazione della conformità di sicurezza

Interporto Rivalta utilizza le certificazioni sia come strumento interno, che come requisito indispensabile per tutti i partner per poter lavorare con l'azienda.

Dal punto di vista interno l'azienda è certificato ISO 9001 per quanto riguarda il sistema di gestione della qualità, ISO 14001 per quanto riguarda il sistema di gestione ambientale e HACCP per quanto riguarda il sistema di gestione dell'igiene, avendo a che fare con diversi prodotti alimentari.

L'azienda inoltre richiede ai propri partner le stesse certificazioni per poter garantire al cliente industriale delle procedure adeguate lungo tutta la filiera.

"Spesso è lo stesso cliente che ci richiede di utilizzare fornitori che abbiamo queste certificazioni. Soprattutto i grossi gruppi che sono molto sensibili alle tematiche legate all'ambiente, impongono che tutta la filiera possegga determinati requisiti e lavori in un certo modo, e il sistema di ispezione e controllo della qualità è molto stringente. Il controllo è quindi doppio, fatto sia da noi che dal nostro cliente". [*]

L'impatto di questa politica è stato individuato sull'inadeguatezza delle procedure sia lato attacchi che fornitura.

Partnership

Per quanto riguarda la tipologia di rapporti con i propri partner, mentre il rapporto con l'operatore ferroviario è forzatamente di lungo periodo essendoci una situazione di quasi monopolio, con i padroncini si cerca di instaurare delle relazioni di lungo periodo.

"Cerchiamo di avere delle partnership con tutti i nostri fornitori. Per fornitori intendo sia i padroncini che quindi effettuano il trasporto su strada ma anche tutti le aziende che ci forniscono le attrezzature per i magazzini, chi ci supporta nella costruzione di magazzini ecc. che per noi sono più importanti dal punto di vista della mole di lavoro gestita. In ogni caso il nostro obiettivo ultimo è quello di fidelizzarli, di utilizzare sempre i soliti per farli crescere con noi. Ovviamente poi anche l'aspetto economico importa, e quindi organizziamo dei bandi di gara con requisiti economici e di qualità del servizio per decidere a chi affidare il lavoro". [*]

L'impatto di questa politica è su tutti i fattori causa legati alla sicurezza da attacchi e fornitura.

[*] Frasi estrapolate dall'intervista a Gian Luca Fossati, ufficio Sales&Marketing di Interporto Rivalta Scrivia

"Le relazioni di lungo periodo ci garantiscono sul fatto che i nostri partner siano adeguati dal punto di vista procedurale e lavorino in un certo modo, oltre al fatto che condividere obiettivi e interessi comuni riduce i casi di collusione lungo la filiera. In più incide anche dal punto di vista dell'integrazione e della visibilità sul partner che sicuramente è molto maggiore rispetto al collaboratore spot". [*]

Per Interporto Rivalta l'altra relazione di lungo periodo importante è quella con il cliente industriale che molto spesso in prima persona impone precise politiche gestionali aell'azienda che poi si impegna a trasferirle a tutti i suoi partner.

Sviluppo della consapevolezza sulla sicurezza con i partner

Come evidenziato nella partnership, Interporto Rivalta ha anche il compito di educare e rendere adeguati tutti gli attori della filiera per poter garantire al cliente industriale un servizio di qualità.

Le procedure possono essere stabilite dall'azienda stessa o dal cliente industriale, e Interporto Rivalta mediante corsi di formazione continua e riunioni periodiche le trasmette a tutta la parte di filiera di cui è responsabile.

L'impatto si rileva quindi a livello operativo, nell'implementazione delle procedure sia lato attacchi che fornitura.

Riduzione della differenza di cultura tra azienda e partner

Oltre ai corsi di formazione, attualmente a livello strutturale Rivalta non organizza incontri periodici o workshop con l'obiettivo di fare squadra con i propri partner.

Focus sul cliente finale

Non esiste un'ottica comune condivisa tra tutti gli attori del trasporto intermodale anche perché non esiste una forma di incentivazione del buon lavoro dell'intera filiera.

Grado di importanza degli strumenti

Gli strumenti più importanti per ottenere performance sicure sono stati individuati tra quelli interni all'azienda come forza lavoro multidisciplinare, collaborazione tra dipendenti, integrità, lealtà dei dipendenti e sviluppo della sicurezza interna sulla sicurezza. Questo perché sono ritenuti gli strumenti indispensabili per fare squadra e creare i presupposti per un lavoro di qualità.

[*] Frasi estrapolate dall'intervista a Gian Luca Fossati, ufficio Sales&Marketing di Interporto Rivalta Scrivia

Oltre a questi è stato individuato il continous improvement perché determinante per progettare procedure sicure.

Peso dei fattori causa

Per quanto riguarda la sicurezza da attacchi le cause principali di una cattiva performace sono la collusione insieme all'errata/mancata implementazione delle procedure.
Lato fornitura l'inadeguatezza del partner ferroviario e l'errata/mancata implementazione delle procedure sono state individuate come cause principali del ritardo al cliente finale, seguite da mancata collaborazione/visibilità e inadeguatezza delle politiche gestionali.

Di seguito è riportata la tabella compilata durante l'intervista.

		SICUREZZA DA ATTACCHI			SICUREZZA DI FORNITURA			
		2	2	1	1	3	3	1
	Lo strumento viene utilizzato in azienda?	Collusione	Errata/mancata implementazione delle procedure	Inadeguatezza delle procedure	Mancata collaborazione / visibilità con i partner	Inadeguatezza partner	Errata/mancata implementazione delle politiche gestionali	Inadeguatezza delle politiche gestionali
Forza lavoro multidisciplinare	**f.**		↓				↓	
Collaborazione tra dipendenti	**f.**	↓	↓				↓	
Integrità, lealtà dei dipendenti	**f.**		↓				↓	
Sviluppo della consapevolezza interna sulla sicurezza	**f.**		↓				↓	
Aspetti soft	**f.**	↓	↓					
Continuous improvement	**n.f.**			↓				↓
Business continuity planning	**f.**			↓				↓
Segnalare incidenti e debolezze	**n.f.**		↓	↓			↓	↓
Knowledge management	**n.f.**	↑↓	↓				↓	
Valutazione della conformità di sicurezza	**f.**			↓				↓
Partnership	**f.**	↓	↓	↓	↓	↓	↓	↓
Sviluppo della consapevolezza sulla sicurezza con i miei partner	**f.**		↓				↓	
Riduzione della differenza di cultura tra aziende e partner	**NO**							
Focus sul cliente	**NO**							

Evidenziati in giallo gli strumenti ritenuti indispensabili per ottenere performance sicure e i principali fattori che causano una minore sicurezza da attacchi e fornitura, la scala utilizzata per i fattori causa è in ordine crescente di importanza.

La risposta "n.f." sull'utilizzo dello strumento in azienda significa che lo strumento viene utilizzato in azienda ma non in maniera standard o formale.

D.8 Marenzana

Tipologia azienda: MTO con padroncini interni

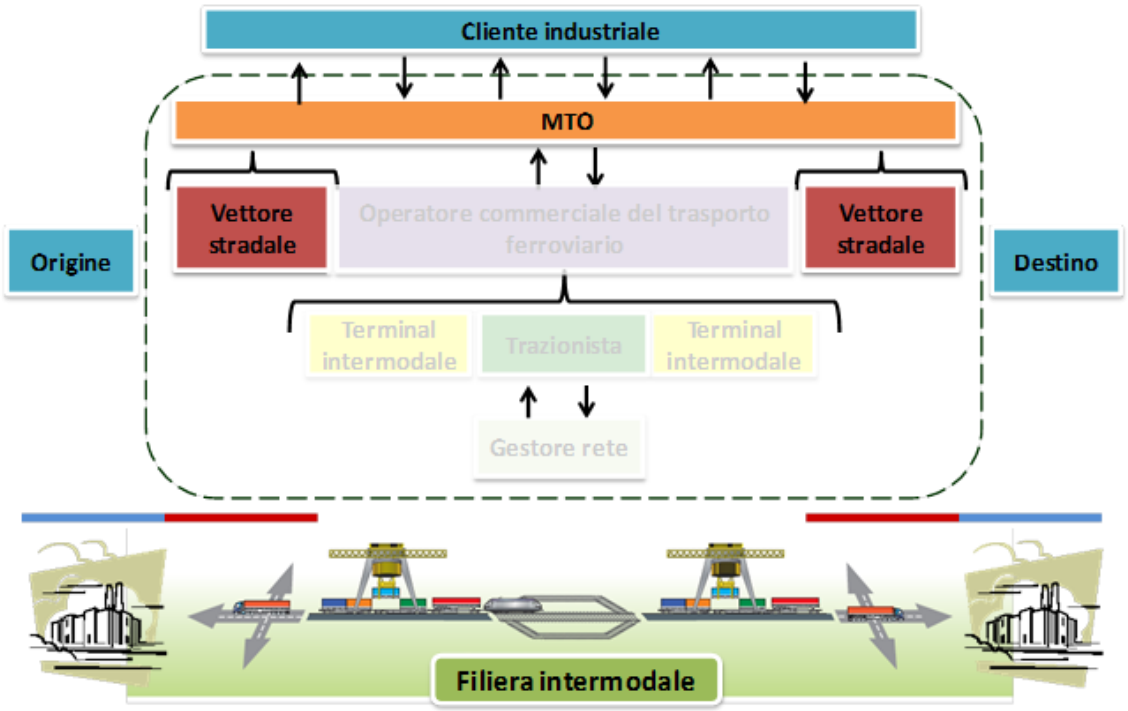
Area di responsabilità diretta: pianificazione del trasporto intermodale, gestione del rapporto cliente/fornitore e trasporto su gomma

Fatturato: 13,5 mln €

Dipendenti: 90 tra cui 70 autisti

Interlocutore: Francesca Doria, Operational Manager

Sede intervista: Uffici di Marenzana presso Novi Ligure (AL)



Premessa

Marenzana SpA è un'azienda operante nel settore dei trasporti multimodali di prodotti chimici sfusi in Europa, ed attualmente è una delle prime aziende italiane di questo specifico settore.

L'azienda offre servizi di trasporto su gomma per servire il mercato domestico, ed un servizio di tipo intermodale per collegamenti internazionali con direttrice principale Olanda-Italia.

Per quanto riguarda il traffico intermodale, di responsabilità diretta è la pianificazione del trasporto, la gestione del rapporto con fornitori e clienti industriali e il trasporto su gomma. L'azienda si affida a operatori ferroviari per il cambio di modalità di trasporto e la trazione su rotaia.

L'azienda sviluppa traffici prevalentemente sulla direttrice Olanda-Italia sfruttando un rapporto di partnership con un'azienda di trasporto multimodale olandese, la RMI.

Nella maggior parte dei casi i tank container vengono caricati in Olanda e spediti via ferro in Italia, per essere scaricati e consegnati al cliente finale, e successivamente essere rispediti vuoti in Olanda.

L'azienda possiede una vasta flotta composta da tank container, cisterne stradali e trattori stradali, guidati esclusivamente da autisti dipendenti. Dispone inoltre di una ventina di subvettori che lavorano su base esclusiva, con mezzi noleggiati a lungo termine ed integrati nel sistema di gestione della qualità aziendale.

Mediante la solida relazione di collaborazione con RMI, Marenzana può offrire ai propri clienti un parco mezzi che comprende ben 1000 tank container, con casse mobili di diversa grandezza e portata, e con possibilità di un controllo satellitare.

Di proprietà di Marenzana sono invece 100 trattori stradali, ai quali si aggiungono quelli dei subvettori partner.

L'azienda si interfaccia da un lato con grosse multinazionali del settore chimico che possono concordare con Marenzana di effettuare un trasporto di tipo intermodale, e dall'altro con un operatore ferroviario che gestisce la tratta su ferro e con un gestore di terminal intermodale che si occupa di effettuare il cambio di modalità di trasporto. L'azienda non ha quindi un contatto diretto con il trazionista ferroviario, responsabilità affidata a chi gestisce la parte di trasporto su rotaia.

L'azienda opera esclusivamente nel settore del trasporto di prodotti chimici sfusi, il più delle volte classificati come merce ADR, che richiedono delle specifiche condizioni di trattamento al fine di evitare rischi di esplosione, incendio o esalazioni tossiche.
Anche per questo motivo il pericolo furti, e più in generale tutto quello che fa parte della sicurezza da attacchi intenzionali, è del tutto assente in azienda, trattando merce non appetibile e difficilmente maneggiabile e asportabile.
Per questo motivo gli attacchi intenzionali non sono stati inclusi negli argomenti dell'intervista.
Il contributo di Francesca Doria offre il punto di vista di chi deve gestire e pianificare un trasporto di tipo intermodale per un'azienda di medio/piccola dimensione che fa della qualità di servizio una delle sue armi principali.

Adozione degli strumenti

Forza lavoro multidisciplinare

Per quanto riguarda la forza lavoro multidisciplinare, il riferimento è agli autisti dipendenti di Marenzana, e dare loro una formazione più ampia rispetto a quelle che sono le loro mansioni operative non rientra nella politica aziendale perché non è ritenuto utile.
Anche allargando il discorso dalla strette mansioni operative, agli autisti non viene data una visione d'insieme dell'intero processo intermodale; per esempio le informazioni sulla merce trasportata sono ridotte allo stretto necessario.
"Agli autisti interessa fino a un certo punto da che cliente poi dovrà andare il container. Loro sanno per quale destinazione devono portare il container, così che possano fare un controllo della prenotazione fatta in precedenza, e questo è importante che lo facciano. Per il resto dar loro una formazione a più ampio spettro non penso sia importante".[*]

Collaborazione tra dipendenti

La collaborazione interna è ritenuta un elemento molto importante, e il riferimento è sia a livello di pianificazione che a livello operativo.
In azienda l'area planning è divisa in tre parti, una che cura i traffici intermodali di tank container, una che cura i trasporti mediante l'autostrada viaggiante alpina e una che cura

[*] Frasi estrapolate dell'intervista a Francesca Doria, Operational Manager di Marenzana

esclusivamente i trasporti su gomma. Anche gli autisti sono assegnati a queste tre aree sulla base del volume medio di traffico da gestire.

*"A ciascuna area assegniamo un numero di autisti, un numero di mezzi, un numero di cisterne ed un numero di pianali. La collaborazione e il lavoro di squadra è fondamentale all'interno di ogni area, ma lo è anche tra le diverse aree perché sulla base delle richieste dei nostri clienti capita spesso di doversi scambiare mezzi e trattori ".**

Pur non essendoci delle politiche formali per incentivare il lavoro di squadra, questo è ritenuto indispensabile soprattutto nel trasferimento di esperienza dagli autisti più esperti a quelli meno.

*"Il lavoro degli autisti non è affatto semplice, soprattutto per il tipo di prodotti con cui entrano in contatto, le particolarità che devono seguire, le procedure che devono rispettare e noi siamo molto rigorosi da questo punto di vista. Quando prendiamo un autista nuovo gli affianchiamo almeno per una settimana un istruttore, per fargli imparare tecniche di guida sicura, per fargli conoscere gli stabilimenti, fargli vedere la messa in pratica delle procedure per lavorare in sicurezza. Poi c'è da dire che selezioniamo gli autisti anche in base alla loro provenienza, per farli rimanere vicino a casa, e quindi loro si specializzano su una tipologia di lavoro relativa ai traffici su una direttrice. Nel caso in cui ci sia l'esigenza di spostare l'autista su un altro tipo di lavoro viene previsto tranquillamente un altro periodo di affiancamento". **

La collaborazione è quindi ritenuta impattare sugli episodi di errata/mancata implementazione delle procedure.

Integrità, lealtà dei dipendenti

Marenzana fornisce un manuale a tutti gli autisti che esplicita le regole di comportamento.

*"Nel manuale è presente un estratto di tutte le politiche della società in termini di non utilizzo di droghe, alcool e vengono dettate delle norme di comportamento che devono seguire sia in sede, sia presso i clienti, che vanno dalla disponibilità alle esigenze del cliente ai dispositivi di sicurezza che devono mettere e quant'altro. Per tutti gli autisti il manuale deve essere trattato come una Bibbia".**

* Frasi estrapolate dell'intervista a Francesca Doria, Operational Manager di Marenzana

L'azienda ha anche un metodo formale per incentivare gli autisti che durante l'anno hanno saputo svolgere un buon lavoro.

"Ogni fine anno facciamo una sorta di pagellina dell'autista, che si basa sul consumo di carburante, su quante assenze ha fatto, su quanto è stato puntuale ed altri fattori. Raccogliamo una valutazione dell'autista da tutte le persone con cui è entrato in contatto, dai planner al responsabile della qualità, ai clienti. Data la pagellina, a questa corrisponde un premio in denaro.

Ultimamente poi ho iniziato a fare analisi sul rispetto di alcune procedure imposte dall'alto come può essere la compilazione di chek-list, e ho proiettato la lista dei migliori tredici autisti nelle nostre riunioni". *

Gli impatti di queste politiche secondo la nostra interlocutrice sono importanti per la motivazione degli autisti con impatto sull'errata/mancata applicazione delle procedure.

Sviluppo della consapevolezza interna sulla sicurezza

Marenzana organizza degli incontri periodici nei quali si parla di sicurezza a 360 gradi.

"Facciamo delle sessioni di formazione con gli autisti una o due volte all'anno. In queste occasioni ci riuniamo e oltre alla formazione rivediamo quelli che sono stati i problemi durante l'anno, le non conformità, i ritardi, le novità sul trasporto ADR. In più chiacchieriamo sul rispetto delle ore di guida, sugli errori che hanno fatto, sulle mancate pause e cose di questo tipo". *

L'impatto di queste iniziative si riscontra direttamente nell'implementazione delle procedure operative ma anche sull'inadeguatezza delle politiche gestionali.

"Lo scopo è di fare in modo che con una formazione insistente anche gli autisti più indisciplinati rispettino le procedure che abbiamo fatto. Capita anche spesso che da questi incontri siano gli autisti che ci danno degli input per migliorare delle procedure". *

Aspetti soft

Marenzana non è dotata formalmente di un codice etico o di un motto o di una vision con specifico richiamo sulla sicurezza.

L'azienda ritiene però che il miglior modo per creare un buon clima aziendale e fidelizzare i propri dipendenti sia con raduni periodici, come le giornate dedicate agli autisti, i "drivers day".

* Frasi estrapolate dell'intervista a Francesca Doria, Operational Manager di Marenzana

"Lo scorso anno abbiamo fatto per la prima volta una giornata dedicata esclusivamente agli autisti. Alla mattina c'è stata una riunione nel quale abbiamo fatto il punto della situazione dell'azienda mentre al pomeriggio dopo aver pranzato tutti insieme siamo andati a fare una gara di go-kart. Credo che queste siano iniziative importanti per far sentire gli autisti parte dell'azienda e per fare gruppo".[*]

Inoltre vengono organizzate un paio di volte all'anno delle giornate di incontro e team-building dedicate a chi lavora in area operativa, amministrativa e in officina.

"Possono essere giornate alle terme, piuttosto che gite in barca a vela o cose di questo tipo. Il nostro è un lavoro molto stressante e spesso siamo sotto pressione per mille motivi. Queste giornate penso che siano fondamentali per ritrovare armonia e spirito di gruppo, e appianare le divergenze che possono emergere nel lavoro quotidiano".[*]

L'impatto di queste iniziative è stato individuato nell'errata/mancata applicazione delle procedure, diretta conseguenza di una maggiore attenzione e motivazione dei dipendenti.

Continous improvement

Marenzana non ha un sistema formale per incentivare i suggerimenti dal lato operativo ma è molto stretto il rapporto tra chi pianifica e gli autisti.

Oltre alle occasioni di incontro prima citate nello sviluppo della consapevolezza interna sulla sicurezza, anche il rapporto con gli autisti è fondamentale per migliorare le politiche gestionali.

"Noi non abbiamo bisogno di formalizzare questo processo. Io con gli autisti parlo ogni giorno e raccolgo le loro lamentele, critiche e suggerimenti in relazione in particolar modo all'aspetto della sicurezza durante le operazioni di carico e scarico ma non solo.

Questo processo è difficile da formalizzare perché gli autisti sono abbastanza allergici ad utilizzare carta e penna e preferiscono sempre e comunque parlare di persona". [*]

Il procedimento è agevolato in Marenzana essendo un'azienda relativamente piccola, nella quale tutte le persone si conoscono, e il rapporto tra operai e chi pianifica è quotidiano.

Business continuity planning

In caso di situazioni impreviste non sono presenti piani d'azione predefiniti da seguire.

[*] Frasi estrapolate dell'intervista a Francesca Doria, Operational Manager di Marenzana

*"Quando accade un imprevisto la prima cosa è che l'autista non prenda iniziative personali e ci contatti al nostro numero d'emergenza che è attivo 24 ore su 24. Nel manuale dell'autista che hanno su tutti i camion ci sono delle indicazioni su cosa fare nel caso di alcune situazione ma principalmente sono indicazioni per la sicurezza dell'autista stesso. Per quanto riguarda la sicurezza di fornitura non abbiamo dei piani prestabiliti e siamo noi dalla pianificazione che decidiamo come intervenire di volta in volta". **

Segnalare incidenti e debolezze

Per quanto riguarda la segnalazione di incidenti o debolezze Marenzana richiede agli autisti di segnalare formalmente pericoli e near messes mediante la compilazione di una chek-list.

*"Abbiamo una procedura con un apposita chek-list che chiediamo sempre e insistentemente agli autisti di compilare ogni volta che vanno in uno stabilimento e si accorgono di qualche cosa che non va bene, che potrebbe essere pericoloso per loro, per il mezzo o per le persone nei paraggi. Il modulo comprende anche uno spazio apposito per la segnalazione dei quasi rischi o incidenti".**

L'utilizzo di queste chek-list è indispensabile per la sicurezza di fornitura, perché sono la base di un processo di miglioramento continuo del processo.

"Abbiamo implementato un sistema per cui teniamo traccia ogni giorno di tutti i ritardi, per qualsivoglia motivo siano successi, e le loro conseguenze. L'intento è quello di raccogliere questi dati per trovare delle possibili azioni correttive basandosi su un'analisi anche quantitativa. Le chek-list sono il punto di partenza per questo processo.

*La cosa più difficile è convincere gli autisti a compilare queste chek-list perché di base sono restii a usare carta e penna. Avendo però 70 autisti da gestire è importante che la segnalazione sia messa per iscritto così che sia più facile da processare". **

Gli impatti di queste segnalazioni sono state individuate utili al miglioramento dei processi ad alto livello, ed anche a individuare le inadeguatezze dei partner d'azienda sia di tipo industriale che dei terminal intermodali.

"Quando la segnalazione di una mancanza di un partner viene trasferita nel sistema viene resa anonima, così che gli autisti si sentano tranquilli nel farla. La segnalazione

* Frasi estrapolate dell'intervista a Francesca Doria, Operational Manager di Marenzana

della causa del ritardo viene poi codificata per rendere più veloci le elaborazioni successive". [*]

Knowledge management

In azienda non è presente un software che formalmente gestisce la conoscenza e la rende disponibile a tutti. Questo processo viene applicato informalmente tramite collaborazione e socializzazione informale.

Valutazione della conformità di sicurezza

Marenzana dalla sua nascita è sempre stata molto attiva in ambito certificazioni; dal 1993 possiede la certificazione ISO 9001 che attesta la qualità del sistema di gestione d'impresa, e dal 1994 ha sposato il progetto SQAS (Safety and Quality Assessment System) per certificare le proprie procedure in ambito sicurezza, qualità e politiche ambientali.

L'azienda inoltre partecipa a vari gruppi di lavoro della ECTA (European Chemical Transport Association) in ambito sicurezza.

Per quanto riguarda la valutazione della conformità dei subvettori che collaborano con Marenzana, il processo di selezione e valutazione è molto rigido.

"Per tutti i subvettori abbiamo una procedura di omologazione e di controllo parecchio stringente. Il processo può essere anche molto lungo e non si conclude fino a che il nostro responsabile della qualità li ritiene idonei per fare i nostri trasporti. Anche per questo abbiamo molti rapporti di lungo periodo con questi partner perché attivare un nuovo processo di omologazione è lungo e dispendioso". [*]

La valutazione della conformità interna è ritenuta importante per migliorare le politiche gestionali d'azienda mentre quella esterna impatta sull'inadeguatezza dei partner di filiera; di riflesso questo strumento garantisce qualità dal punto di vista dell'implementazione delle procedure operative.

Partnership

Per l'azienda l'instaurazione di rapporti lungo periodo è fondamentale non tanto con gli attori con i quali si interfaccia per la parte ferroviaria (terminal e vettori ferroviari), quanto per i subvettori che l'azienda utilizza per il trasporto stradale e verso il partner olandese RMI che spedisce container carichi dall'olanda con destinazione finale in Italia.

[*] Frasi estrapolate dell'intervista a Francesca Doria, Operational Manager di Marenzana

Questa politica ha l'obiettivo ultimo di garantire affidabilità e qualità al cliente finale.
Con i subvettori una relazione di lungo periodo è necessaria essendo il processo di selezione molto lungo e dispendioso, e sfruttandoli poi in maniera quasi esclusiva e integrata, in quanto inseriti nel sistema di gestione della qualità aziendale.
Marenzana non fa quindi differenze tra i propri autisti e quelli dei subvettori, trattandoli tutti allo stesso modo.
La partnership oltre che sulla garanzia del servizio offerto è ritenuta importante per assicurare integrazione e visibilità sull'operato del partner olandese.
"Nella pratica è come se fossimo una stessa azienda. Abbiamo varie procedure di controllo sulle partenze e arrivi dei container, sulle date di carico e scarico e ogni giorno ci interfacciamo con loro per organizzare i trasporti. Abbiamo un sistema di gestione condiviso che ci garantisce la massima sicurezza sull'organizzazione del trasporto. Noi possiamo anche indicare a loro cosa caricare in maniera urgente, loro possono fare la stessa cosa con noi per lo scarico. La comunicazione sicuramente non manca".[*]

Sviluppo della consapevolezza sulla sicurezza con i partner

Per quanto riguarda il rapporto con i padroncini, Marenzana oltre al processo di omologazione iniziale si pone come promotore delle iniziative di formazione continua sulla base delle informazioni ricavate dal controllo di qualità.
Rispetto ai contratti, oltre alle clausole di sicurezza e di livello di servizio minimo da garantire, sono presenti delle penali riferite alla prestazioni offerte.
"Non abbiamo delle penali riferite al ritardo causato, ma per i subvettori ai quali ci affidiamo più spesso richiedendo tutti i giorni 5-6 macchine, abbiamo fissato delle penali qualora non riuscissero a garantirci un numero minimo di macchine, mettendoci così in grossa difficoltà". [*]
Gli impatti di questa politica sono stati individuati sia ad alto livello per quanto riguarda l'inadeguatezza del partner e delle sue politiche gestionali, sia a livello operativo per l'errata/mancata implementazione delle procedure.

[*] Frasi estrapolate dell'intervista a Francesca Doria, Operational Manager di Marenzana

Riduzione della differenza di cultura tra azienda e partner

Marenzana, come detto in precedenza a proposito dello sviluppo della consapevolezza interna sulla sicurezza, organizza degli incontri periodici con gli autisti per fare formazione e creare un momento di incontro informale.

A questi incontri sono invitati anche i padroncini esterni che vengono trattati come i propri dipendenti con l'idea di fare squadra.

Inoltre con riferimento al partner olandese RIM, vengono organizzate delle giornate di incontro.

"Una volta all'anno ci incontriamo o in Italia o in Olanda e passiamo una weekend insieme. Lo scopo è quello di rivedere le problematiche che ci possono essere state durante l'anno, magari che riguardano la comunicazione, e passare un pochino di tempo insieme aldilà di quello che è il lavoro di tutti i giorni. Creare uno spirito di squadra è fondamentale e credo anzi che dovremmo aumentare queste occasioni d'incontro, perché forse una volta all'anno è troppo poco". [*]

Questo strumento, oltre agli impatti già individuati nello sviluppo della consapevolezza interna sulla sicurezza, ha effetti anche sull'inadeguatezza del partner.

Focus sul cliente finale

La visione d'insieme secondo la nostra interlocutrice è presente, ma solo all'interno dell'area di responsabilità di ogni attore della filiera. Non esiste quindi un'integrazione tale da far si che tutti gli attori della filiera lavorino con un'ottica comune.

"Noi vediamo il treno come un mezzo, ne conosciamo gli orari di partenza e arrivo, il numero di treni al giorno, le tracce ecc., però non lo riteniamo parte integrante del nostro processo. Ci limitiamo a fare riservazioni ed eventualmente dei reclami per mancato servizio". [*]

Grado di importanza degli strumenti

Tra gli strumenti analizzati quelli ritenuti indispensabili per ottenere performance sicure sono stati individuati nella collaborazione tra dipendenti, sviluppo della consapevolezza interna sulla sicurezza, segnalazione di incidenti e debolezze e partnership.

[*] Frasi estrapolate dell'intervista a Francesca Doria, Operational Manager di Marenzana

Peso dei fattori causa

Per quanto riguarda la sicurezza di fornitura l'inadeguatezza del partner è stata individuata come la causa principale dei ritardi provocati al cliente finale. Come secondo fattore causa è stata individuata la mancanza di collaborazione e visibilità con i partner e successivamente l'errata o mancata implementazione delle procedure operative el'inadeguatezza delle politiche gestionali.

Di seguito è riportata la tabella compilata durante l'intervista.

		SICUREZZA DA ATTACCHI			SICUREZZA DI FORNITURA			
					3	4	2	1
	Lo strumento viene utilizzato in azienda?	Collusione	Errata/mancata implementazione delle procedure	Inadeguatezza delle procedure	Mancata collaborazione / visibilità con i partner	Inadeguatezza partner	Errata/mancata implementazione delle politiche gestionali	Inadeguatezza delle politiche gestionali
Forza lavoro multidisciplinare	**NO**							
Collaborazione tra dipendenti	**n.f.**						↓	
Integrità, lealtà dei dipendenti	**f.**						↓	
Sviluppo della consapevolezza interna sulla sicurezza	**f.**						↓	↓
Aspetti soft	**n.f.**						↓	
Continuous improvement	**n.f.**							↓
Business continuity planning	**NO**							
Segnalare incidenti e debolezze	**f.**					↓		↓
Knowledge management	**NO**							
Valutazione della conformità di sicurezza	**f.**					↓	↓	↓
Partnership	**f.**				↓	↓	↓	
Sviluppo della consapevolezza sulla sicurezza con i miei partner	**f.**					↓	↓	↓
Riduzione della differenza di cultura tra aziende e partner	**f.**						↓	↓
Focus sul cliente	**NO**							

Evidenziati in giallo gli strumenti ritenuti indispensabili per ottenere performance sicure e i principali fattori che causano una minore sicurezza da attacchi e fornitura, la scala utilizzata per i fattori causa è in ordine crescente di importanza.

La risposta "n.f." sull'utilizzo dello strumento in azienda significa che lo strumento viene utilizzato in azienda ma non in maniera standard o formale.

D.9 Magazzini Desio Brianza M.D.B

Tipologia azienda : MTO puro e gestore di un terminal intermodale

Area di responsabilità diretta : pianificazione del trasporto intermodale, cambio di modalità di traporto

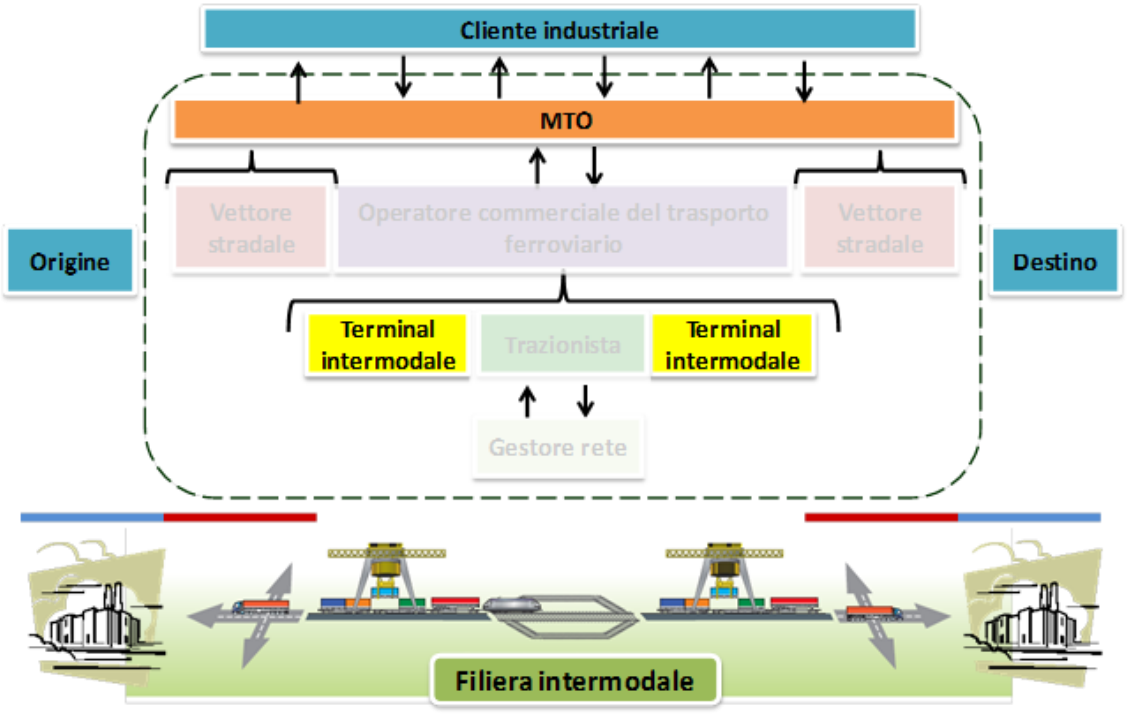
Proprietà : Express-Italia (società controllata al 100% delle ferrovie austriache)

Fatturato: 11 mln € (2008)

Dipendenti: 36

Interlocutore : Bruno Carbonin, Direttore

Sede intervista : Uffici di MDB presso la base logistica di Desio (MB)



Premessa

Magazzini Desio Brianza è una società che nasce alla fine degli anni ‘80 da un progetto di recupero di una zona industriale dismessa. La sua caratteristica fondamentale è il fatto di essere dotata di un raccordo diretto sulla linea ferroviaria Milano-Chiasso, che è la principale direttrice tra l’Italia e il Nord Europa.

MDB è una medio-piccola impresa che abbina i servizi tipici di un terminal intermodale alla gestione e supervisione del trasporto iniziale e finale su strada (effettuato con l’ausilio di padroncini esterni).

Di responsabilità diretta di MDB sono anche le operazioni di manovra e scambio dei vagoni sul raccordo ferroviario, fino alla cessione del mezzo all’operatore ferroviario che si occupa della trazione su rotaia.

Attualmente MDB ha l’intero personale (36 persone) dipendente, dislocato tra gli uffici, i magazzini e il raccordo ferroviario di Desio.

MDB offre un servizio di trasporto intermodale, nel quale ogni cambio di modalità di trasporto avviene con rottura del carico. I vagoni in arrivo vengono terminalizzati, quindi la merce viene scaricata e stoccata nei magazzini adiacenti, per poi essere ricaricata sui camion per il trasporto dell’ultimo miglio per raggiungere il cliente finale.

L’azienda tratta con due tipologie di clienti; da un lato le aziende ferroviarie e dell’altro clienti industriali.

I grossi operatori ferroviari (con funzione anche di MTO) si occupano del rapporto con il cliente finale e del trasporto su rotaia, e sfruttano la base logistica MDB per il cambio di modalità e il trasporto su strada dell’ultimo miglio, così da poter offrire un trasporto franco stabilimento di consegna. In questo caso MDB interagisce unicamente con il partner ferroviario ma non ha contatti con il cliente finale.

Per quanto riguarda i clienti industriali è invece MDB che si pone come unico interlocutore con responsabilità di supervisione dell’intero processo di trasporto.

MDB non possiede camion per il trasporto su gomma e si affida a società esterne, così come per quanto riguarda la trazione ferroviaria.

L’azienda si occupa prevalentemente del trasporto e dello stoccaggio di acciaio (in coils fino a 35 tonnellate) e carta (stoccata in bobine che arrivano a pesare fino a 6 tonnellate) ed in misura minore di prodotti chimici.

Trattando prevalentemente merce industriale pesante, di bassa appetibilità e che necessita di apposite attrezzature per essere maneggiata, il fenomeno dei furti o in

generale degli attacchi intenzionali non è mai stato un reale problema per MDB. L'azienda è dotata di videosorveglianza, di un sistema di sicurezza e di un'assicurazione che copre eventuali furti fino alla consegna al cliente finale, ma il problema è assolutamente relativo.

Per questo motivo gli attacchi intenzionali non sono stati inclusi negli argomenti dell'intervista.

Il contributo di Bruno Carbonin offre un punto di vista a 360 gradi sull'operato di una base logistica di dimensioni medio-piccole.

Adozione degli strumenti

Forza lavoro multidisciplinare

"Il mio obiettivo ideale sarebbe quello di avere degli operatori jolly, che diano meno vincoli nell'utilizzo delle persone e che abbiano la competenza per poter gestire varie tipologie di problematiche. Ma non tutti hanno la capacità di fare tutto. Per esempio i piloti dei locomotori devono avere un'abilitazione specifica rilasciata dalle ferrovie e si occupano esclusivamente del trasporto merce sul raccordo ferroviario".[*]

Tralasciando i piloti dei locomotori e gli addetti ai carrelli elevatori che devono sollevare coils fino a 35 tonnellate, il resto del personale è intercambiabile ed è formato per poter gestire l'intero processo di competenza di MDB. Questo è possibile anche perché il processo è relativamente semplice.

"I nostri operatori non vedono solo il pezzettino del processo come accade nelle aziende di produzione anche perché essendo il nostro processo semplice le persone sanno tutto di tutto. Questo aspetto secondo me è importante perché avere una visione d'insieme, e non solamente limitata alla propria area di competenza, stimola e motiva meglio il personale". [*]

Collaborazione tra dipendenti

La collaborazione interna è un elemento imprescindibile, e non averla è causa di cattive performance dell'azienda.

"La collaborazione è fondamentale ed è governata dalla buona comunicazione interna. Il rapporto interpersonale dei miei dipendenti fuori dall'ambiente di lavoro non è di mia competenza, ma durante l'orario di lavoro è un peccato mortale non far circolare

[*] Frasi estrapolate dell'intervista a Bruno Carbonin, direttore di MDB

*le informazioni e le esperienze. Uno dei miei compiti è anche quello di favorire la comunicazione tra le persone".**

Entrando nello specifico di alcuni metodi operativi per stimolare e favorire la collaborazione, il lavoro in squadra è considerato un elemento determinante.

"Il riferimento al team è sempre importante, perché alla fine è sempre la squadra che produce o meno dei risultati. Per questo motivo abbiamo creato degli incentivi, che per il momento non sono ancora estesi a tutto il personale, e che vanno a premiare il buon lavoro di squadra.

*Attualmente questi incentivi sono presenti per il livello intermedio, quadro e dirigente, sulla base del modello MbO (Management by Objectives) che stiamo applicando da un paio di anni e che assegna degli obiettivi individuali e di squadra rispetto ad una determinata mansione. Sulla base poi degli obiettivi raggiunti o meno, viene assegnato un premio a fine anno."**

L'impatto principale della collaborazione è diretto verso l'errata/mancata implementazione delle procedure operative, come per esempio negli orari di cambio turno.

*"Abbiamo definito i turni di lavoro con orari 6-14 e 12-20 in modo tale da consentire al personale di scambiarsi le consegne fra mattina e pomeriggio. Inoltre il capo turno del pomeriggio deve ogni sera aggiornarsi con quello del mattino successivo per stabilire il lavoro da effettuare il giorno seguente". **

Integrità, lealtà dei dipendenti

MDB attualmente non ha policy di comportamento o programmi per premiare l'integrità e la fedeltà dei dipendenti. Nel futuro però, con l'estensione del modello MbO a tutto il personale d'azienda, anche queste tematiche potrebbero entrare a far parte della metodologia per elargire o meno un premio ai dipendenti a fine anno.

Sviluppo della consapevolezza interna sulla sicurezza

MDB oltre alla formazione iniziale e a quella richiesta dalla legge fa svolgere ai suoi dipendenti dei corsi promossi dalle ASL sulla sicurezza sul lavoro (safety).

Per quanto riguarda la security vengono effettuate delle riunioni che coinvolgono tutto il personale.

"Quando necessario facciamo delle riunioni per spiegare le logiche aziendali in maniera che tutti possano capire al meglio gli obiettivi. Inoltre aggiorniamo i

* Frasi estrapolate dell'intervista a Bruno Carbonin, direttore di MDB

dipendenti in caso di cambiamenti aziendali e sulle nuove problematiche che di volta in volta emergono, dando una comunicazione scritta al termine della riunione e appendendo in bacheca gli avvisi più importanti.
Ovviamente molto dipende anche dal tipo di problematica: se è una questione di poco rilievo informo il personale in maniera informale, altrimenti convoco una riunione".[*]
L'impatto di queste iniziative si riscontra nell'implementazione delle pratiche di lavoro quotidiano. *"Gli operatori sono più consapevoli di cosa devono fare in casi particolari, e il lavoro fluisce meglio".* [*]

Aspetti soft

In azienda non è presente un codice etico/codice di condotta o un motto con specifico richiamo alla sicurezza.
Come detto precedentemente quando necessario vengono organizzate delle riunioni nelle quali sono spiegati gli obiettivi e le politiche aziendali.
"Attualmente non abbiamo strumenti di questo tipo. Nelle grandi aziende vedo che questi codici si stanno diffondendo in maniera molto rapida e probabilmente fra qualche anno potremmo ereditare quello della nostra casa madre (riferimento alle ferrovie austriache).
In ogni caso penso che questo tipo di codici nelle grandi aziende possano avere un impatto sulla motivazione dei dipendenti, ma per un'azienda come la nostra la comunicazione e il rapporto personale è sicuramente più importante". [*]

Continous improvement

La direzione MDB richiede che i propri dipendenti diano dei suggerimenti che possano portare dei benefici a tutti i livelli.
"Vivendo la quotidianità operativa loro rilevano quali possono essere delle migliorie organizzative e a volte le mettiamo in pratica. I suggerimenti sono molto importanti perché loro hanno l'esperienza diretta. Si tratta di capirla e convertirla in un miglioramento reale". [*]
Questo processo è agevolato in MDB essendo un'azienda relativamente piccola e nella quale tutte le persone si conoscono, e il rapporto tra operai e dirigenza è molto stretto.
Questo processo non è ancora formale e non porta ad un incentivo non essendo il livello operativo ancora compreso nel modello MbO. L'idea futura è però quella di estendere il

[*] Frasi estrapolate dell'intervista a Bruno Carbonin, direttore di MDB

modello a tutti i dipendenti di MDB e far si che queste iniziative vengano riconosciute e portino ad un premio a fine anno.

Business continuity planning

In caso di situazioni impreviste non sono presenti piani d'azione alternativi da seguire.

*"Quando accade un fatto del genere se ne discute prima a livello teorico e poi con le persone che agiscono in quel settore per capire la strategia migliore da seguire". **

Segnalare incidenti e debolezze

Per quanto riguarda la segnalazione di incidenti o debolezze MDB si riferisce principalmente al controllo della merce in arrivo e al controllo/manutenzione dell'attrezzatura.

*"In azienda abbiamo una persona che cura esclusivamente le manutenzioni ed esiste un form di segnalazione formale ove previsto dalla legge. In ogni caso facciamo tagliandi di manutenzione preventiva per evitare problemi all'attrezzatura che possono provocare un fermo della produzione". **

Le segnalazioni riguardanti l'attrezzatura, comprendendo le situazioni di near messes, sono ritenute molto importanti, e vengono riportate in maniera informale senza l'ausilio di una procedura standard.

*"In questi casi ne discutiamo con le persone in maniera diretta perché è utile capire bene perché è avvenuta questa situazione e fare in modo che non avvenga più". **

Per una piccola azienda come MDB è più semplice e probabilmente più efficace avere un contatto diretto con gli operatori piuttosto che implementare un sistema formale di segnalazione e gestione delle problematiche. Gli impatti di queste segnalazioni vengono individuate utili sia al miglioramento dell'implementazione delle procedure operative che nella definizione dei processi ad alto livello.

Per le segnalazioni riguardanti problematiche della merce in arrivo esiste un procedimento molto formalizzato per motivi prevalentemente assicurativi.

*"Se la merce in arrivo presenta delle avarie esiste una procedura che prevede l'immissione di riserve sul documento di trasporto, le foto, l'avviso al cliente (mittente) e la richiesta di intervento per la verbalizzazione e per stabilire l'entità e la causa del danno. Fare bene tutti i passi della procedura è importante per evitare di accollarci costi non di nostra competenza". **

* Frasi estrapolate dell'intervista a Bruno Carbonin, direttore di MDB

Gli impatti di queste segnalazioni vengono ritenuti utili oltre che per l'aspetto legale/assicurativo, anche per aiutare il mittente (le ferrovie) a capire la tipologia di danno ed offrire un sevizio qualitativamente più adeguato.

Knowledge management

L'azienda, data anche la sua piccola dimensione, vive e cresce in base all'esperienza maturata giorno per giorno dai suoi dipendenti. Non è presente un software che formalmente gestisce la conoscenza e la rende disponibile a tutti, processo che avviene quotidianamente nelle giornate di lavoro.

"Solitamente alle persone di livello intermedio o alto, prossime a lasciare il lavoro, si fa un periodo di affiancamento con chi andrà a sostituirle, per permettere la trasmissione di quelle piccole esperienze che non è possibile insegnare seduti intorno ad un tavolo. Licenziare in tronco un dirigente o un quadro e non dare continuità al suo lavoro è un patrimonio che va sprecato".[*]

Valutazione della conformità di sicurezza

MDB possiede la certificazione ISO 9001 che attesta la qualità del sistema di gestione d'impresa. Inoltre in ottica di gestione del rischio il processo di controllo è informale e continuo.

"Avviene a tutti i livelli dell'azienda. Non abbiamo un processo strutturato per mappare e migliorare i nostri punti deboli, anche perché data la semplicità del nostro processo probabilmente sarebbe uno sforzo non produttivo".[*]

Il controllo del processo è il punto di partenza per poter apportare migliorie sia a livello operativo che a livello più alto, e spesso si estende anche ai partner di filiera.

"I nostri fornitori più importanti sono i trasportatori, sia su strada che su rotaia. Abbiamo un ufficio di due persone che cura questi due settori e che riceve report via mail o feedback via voce continui. Quando si riscontra un problema io vengo subito informato della situazione e a seconda della gravità me ne occupo personalmente o delego ad un mio collega".[*]

Partnership

Per garantire affidabilità al cliente finale MDB ritiene che le partnership siano un aspetto fondamentale.

[*] Frasi estrapolate dell'intervista a Bruno Carbonin, direttore di MDB

"Per quanto riguarda il trasporto su gomma abbiamo un rapporto di lungo periodo con una casa di spedizioni che ci copre circa l'80% della domanda, e con la quale negli anni abbiamo instaurato un rapporto più che consolidato. Dati gli anni di collaborazione siamo certi della loro qualità di servizio e per questo gli concediamo più flessibilità sulla tariffa, e spesso gli riconosciamo un qualcosina in più del dovuto dal punto di vista economico".[*]

La partnership oltre che sulla garanzia del servizio offerto è ritenuta importante per assicurare integrazione e visibilità sull'operato del partner.

"Non abbiamo un sistema di tracking and tracing condiviso con i nostri padroncini, e quando il cliente finale richiede informazioni, ci rivolgiamo direttamente ai nostri collaboratori tramite telefono o mail. Ovviamente con la casa di spedizioni con cui abbiamo una partnership questo processo è quotidiano ed è molto più fluido e veloce rispetto ai collaboratori spot con cui facciamo più fatica ad ottenere precise informazioni".[*]

Sviluppo della consapevolezza sulla sicurezza con i partner

Per quanto riguarda il rapporto con i padroncini, MDB si pone come promotore delle iniziative di formazione continua sulla base delle esigenze del cliente finale.

"Ogni anno facciamo delle valutazioni in base ai criteri della certificazione di qualità, e vengono fatte delle azioni correttive per il ripristino della qualità. Inoltre costantemente, sulla base delle indicazioni che arrivano dal cliente finale, li istruiamo sulle nuove procedure da svolgere e sul nuovo servizio da offrire.

Organizziamo inoltre delle riunioni quando cambiano le normative per il trasporto imposte dalla legge. Per esempio ultimamente abbiamo avuto una riunione per informarli sull'adeguamento delle forniture di sicurezza come l'elmetto, i pantaloni lunghi e le scarpe anti-infortunistiche per poter entrare in magazzino".[*]

Riduzione della differenza di cultura tra azienda e partner

Per quanto riguarda il rapporto tra MDB e i suoi principali partner, le riunioni organizzate durante l'anno sono importanti oltre che per gli aspetti economici/contrattuali e di aggiornamento delle normative, anche per migliorare il processo di integrazione e collaborazione tra le aziende.

[*] Frasi estrapolate dell'intervista a Bruno Carbonin, direttore di MDB

*"La socializzazione informale è fondamentale per costruire un rapporto affidabile e duraturo con i nostri partner".**

Focus sul cliente finale

Il maggiore problema di MDB per quanto riguarda il servizio al cliente finale è riuscire a definire con chiarezza la propria area di competenza. Questo per poter essere valutati effettivamente sul proprio business.

"Nel passato abbiamo avuto delle lamentele da parte del cliente finale per disservizi che in realtà non competevano a noi, ma alla rete ferroviaria. La comunicazione in questo senso è importante, ed attualmente, anche dopo una lamentala formale alle ferrovie, abbiamo definito ai clienti la nostra area di responsabilità nella filiera". *

Il focus sul cliente è considerata una prospettiva utile per aumentare l'integrazione e la collaborazione tra i partner di filiera.

In ogni caso non esiste ancora la possibilità che il cliente riconosca degli incentivi di filiera da distribuire tra i diversi attori.

Grado di importanza degli strumenti

Tra gli strumenti analizzati quelli ritenuti indispensabili per ottenere performance sicure sono stati individuati nella forza lavoro multidisciplinare, nella collaborazione tra dipendenti, nel segnalare incidenti e debolezze e nella costruzioni di partnership.

Altri strumenti ritenuti importanti ma in maniera minore sono l'integrità a lealtà dei dipendenti, lo sviluppo della consapevolezza interna sulla sicurezza, il continous improvement e la valutazione della conformità di sicurezza.

Peso dei fattori causa

Per quanto riguarda la sicurezza di fornitura l'inadeguatezza del partner è stata individuata come la causa principale dei ritardi provocati al cliente finale. Come secondo fattore causa è stata individuata la mancanza di collaborazione e visibilità con i partner e successivamente l'inadeguatezza delle politiche gestionali e l'errata o mancata implementazione delle procedure operative.

Di seguito è riportata la tabella compilata durante l'intervista.

* Frasi estrapolate dell'intervista a Bruno Carbonin, direttore di MDB

		SICUREZZA DA ATTACCHI			SICUREZZA DI FORNITURA			
					3	4	1	2
	Lo strumento viene utilizzato in azienda?	Collusione	Errata/mancata implementazione delle procedure	Inadeguatezza delle procedure	Mancata collaborazione / visibilità con i partner	Inadeguatezza partner	Errata/mancata implementazione delle politiche gestionali	Inadeguatezza delle politiche gestionali
Forza lavoro multidisciplinare	**f.**						↓	
Collaborazione tra dipendenti	**f.**						↓	
Integrità, lealtà dei dipendenti	**NO**							
Sviluppo della consapevolezza interna sulla sicurezza	**f.**						↓	
Aspetti soft	**NO**							
Continuous improvement	**n.f.**						↓	↓
Business continuity planning	**NO**							
Segnalare incidenti e debolezze	**n.f.**					↓	↓	↓
Knowledge management	**NO**							
Valutazione della conformità di sicurezza	**n.f.**					↓	↓	↓
Partnership	**f.**				↓		↓	
Sviluppo della consapevolezza sulla sicurezza con i miei partner	**f.**					↓	↓	
Riduzione della differenza di cultura tra aziende e partner	**n.f.**				↓			
Focus sul cliente	**NO**							

Evidenziati in giallo gli strumenti ritenuti indispensabili per ottenere performance sicure e i principali fattori che causano una minore sicurezza da attacchi e fornitura, la scala utilizzata per i fattori causa è in ordine crescente di importanza.

La risposta "n.f." sull'utilizzo dello strumento in azienda significa che lo strumento viene utilizzato in azienda ma non in maniera standard o formale.

D.10 Sogemar

Tipologia azienda: operatore commerciale del trasporto ferroviario, terminal intermodale, MTO.

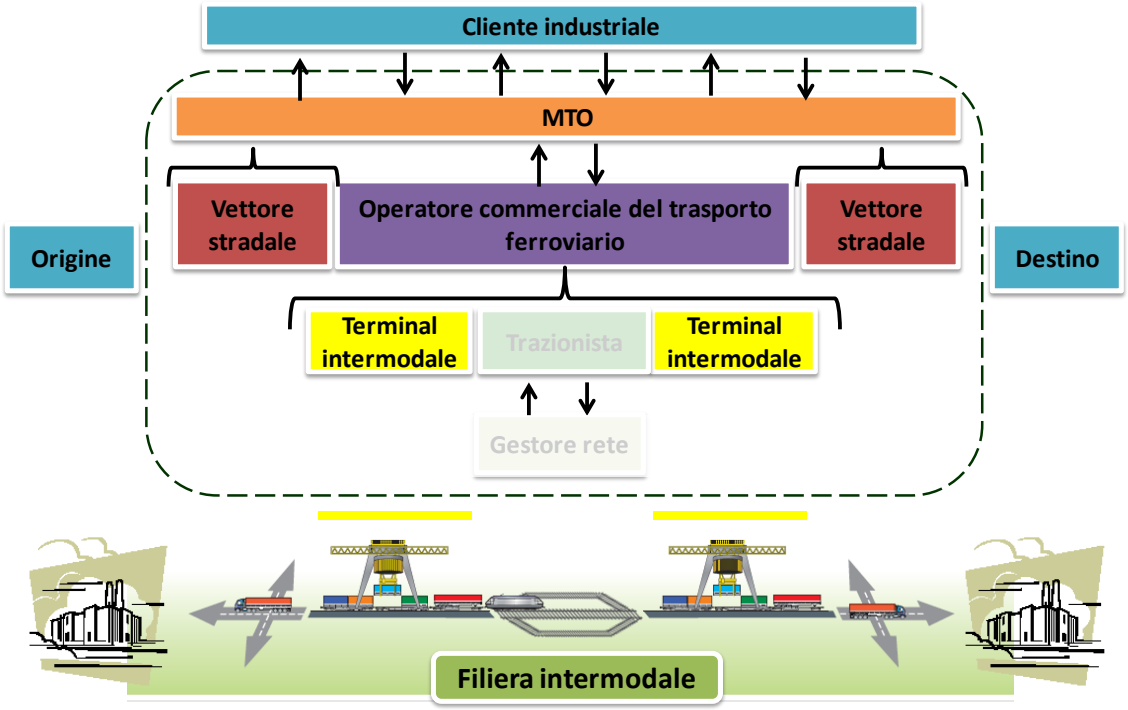
Area di responsabilità diretta: pratiche doganali, stoccaggio, cambio di modalità di trasporto e pianificazione del trasporto continentale (ferroviario e stradale).

Fatturato: 56 mln €

Dipendenti: 150

Interlocutore: Fabrizio Filippi, Direttore operativo

Sede intervista: Uffici di Sogemar S.p.A. c/o Melzo (MI)



Premessa

Sogemar spa fa parte del gruppo Eurokai KGaA che, attraverso le sue due società Eurogate e Contship Italia, opera e controlla il più grande network di terminal container d'Europa. La sede di Eurokai KGaA è ad Amburgo e il focus del gruppo è la gestione e l'esecuzione dei trasporti marittimi. A conferma di ciò vi è la presenza del gruppo nel mare del Nord con i porti di Amburgo, Bremerhaven e Wilhelmshaven; nel mar Baltico con il porto di Ust-luga vicino San Pietroburgo e nel Mediterraneo con i porti di Lisbona, Cagliari, Genova, La Spezia, Gioia Tauro, Ravenna e Tangeri (il quale è attivo da un anno).

Sogemar è controllata al 100% da Contship Italia e la sua attività principale dal 1990 è quella di offrire servizi intermodali, in particolare si occupa di evacuare il più velocemente possibile i porti portando la merce nelle aree produttive. Gestisce direttamente tre terminal di proprietà a Rho, Melzo e Dinazzano (RE) e si appoggia ad altri terminal intermodali a Padova e Bologna. Scelta strategica di Sogemar è stata quella di integrarsi verticalmente all'interno della filiera intermodale creando (in collaborazione con Ferrovie Emilia Romagna) la società Oceanogate che si occuperà della trazione ferroviaria. I clienti di Sogemar sono le compagnie di navigazione le quali stipulano i contratti di resa con i clienti industriali. Come sottolineato dal direttore Fabrizio Filippi però *"di solito dal cliente si va in due: la compagnia di navigazione, e noi. Così si entra subito nel merito per quanto riguarda i servizi franco inland e franco destino, infatti negli ultimi anni le compagnie di navigazione tendono ad offrire un servizio che comprende anche il trasporto finale su terra e non solo la tratta marittima, qui entriamo in gioco noi."*

Facendo capo ad una holding così composta, Sogemar oltre a lavorare a stretto contatto con i vettori marittimi ne estende i loro servizi. Si occupa infatti sia delle attività tipiche dei terminal portuali, come le pratiche doganali, sia di tutte le attività di trasbordo, deposito e movimentazione dei container. Sogemar si affida inoltre ad autisti dipendenti e ad una fitta rete di padroncini (ognuno dei quali possiede anche 50 camion in franchising) per effettuare il trasporto dell'ultimo miglio su gomma.

Attualmente Sogemar è anche proprietaria dei carri ferroviari con cui compone i treni da inviare ai terminal di destinazione.

L'infrastruttura che abbiamo visitato a Melzo si estende su un'area di circa 145.000 m^2 con all'interno 2,2 km di binari interni e 3 km per l'area di composizione dei treni (shunting) con una capacità di movimentazione di circa 250.000 TEU l'anno.
Tutta la superficie è dotata di un sistema di allarme e sorveglianza. L'intera azienda impiega una forza lavoro pari a 150 persone.
Il contributo di Fabrizio Filippi offre una visione chiara e completa del lavoro svolto all'interno di un polo logistico e intermodale tra i più integrati nel panorama europeo.

Adozione degli strumenti

Forza lavoro multidisciplinare

L'azienda si impegna nel formare forza lavoro multidisciplinare.
"Non vogliamo specializzare i dipendenti affinché sappiano lavorare solo sulla gestione dei contenitori vuoti o solo sulla logistica internazionale, che prevede l'utilizzo di casse mobili anziché semirimorchi. Abbiamo 4 logistiche differenti che richiedono processi diversi: gestione del parco vuoti, trasporto marittimo, continentale o internazionale. Ogni operatore deve saper gestire tutte queste differenti situazioni". *
Sono inoltre tutti formati e sensibili su temi di sicurezza infatti *"il gruista anche se è a una certa distanza rispetto al checker si accorge subito se il sigillo è messo male."* *
L'impatto è sull'operatività, formando gli operai su competenze ad ampio spettro è più facile individuare anomalie durante l'implementazione delle procedure riducendo così i casi di mancata o errata implementazione sia per quanto riguarda i furti che i ritardi.

Collaborazione tra dipendenti

Sogemar ha un'attenzione particolare per il lavoro di squadra.
"Vengono tutti gestiti a team, a blocchi, noi abbiamo delle squadre (squadra blu, gialla, verde, ecc) e c'è molta integrazione e competizione tra di loro." *
La conformazione del gruppo inoltre non è statica ma si evolve tenendo conto del grado di maturità dei singoli individui.
"Ovviamente la conformazione del team può cambiare in funzione delle esigenze della persona e della sua crescita, esiste una persona all'interno della funzione Risorse Umane che si occupa proprio di questo." *
A testimonianza della forte attenzione su questo aspetto viene applicato un incentivo economico coerente

* Frasi estrapolate dall'intervista a Fabrizio Filippi, Direttore Operativo di Sogemar

"*Esiste inoltre un meccanismo di incentivazione di gruppo."* [*]

L'impatto è sulla motivazione dei dipendenti i quali hanno maggior attenzione ad implementare correttamente le procedure sia lato attacchi che fornitura.

Integrità, lealtà dei dipendenti

L'attenzione all'integrità e alla lealtà delle persone si avverte subito in Sogemar; appena si entra nella sala riunioni, su una parete, c'è uno slogan che sottolinea il fatto che un'azienda è composta da persone e sono queste che determinano le buone o le cattive prestazioni.

"Come testimonia la scritta su quella parete (people first!) *noi siamo molto attenti alle persone, ad esempio l'altro giorno c'è stata una festa per una persona che è andata in pensione dopo 40 anni di Sogemar, di questi tempi in cui le imprese si muovono molto sul mercato del lavoro è una cosa rara".* [*]

Sogemar non ha mai subito un furto interno dal 1959, questo vuol dire che i dipendenti avvertendo questa attenzione nei loro confronti, sono responsabili e motivati. Gli impatti sono quindi su collusione e errata/mancata implementazione delle procedure sia lato attacchi che fornitura.

Sviluppo della consapevolezza interna sulla sicurezza

In azienda esiste un meccanismo formale per trasmettere il concetto di sicurezza e la sua importanza.

"Ogni 3 mesi facciamo una riunione con tutte le persone del piazzale, e non è facile mettere insieme tutte quelle persone in un ufficio o in un albergo, lì vengono spiegati tutti i risultati dell'azienda, i risultati operativi, si analizzano le richieste dei 3 mesi prima, si mostra dove siamo e dove vogliamo arrivare e si segnano le nuove richieste. In più ci sono le riunioni settimanali con i capireparto. L'attenzione alla sicurezza è massima." [*]

Spiegando in modo dettagliato come cambieranno e il perché vengono cambiate le procedure, l'impatto che si ha è sulla loro implementazione operativa, questa migliora sia lato attacchi che lato fornitura.

In Sogemar esiste una figura di Buildings Maintenance, Quality, Safety, Security & Environment Manager con responsabilità specifiche sulla sicurezza.

[*] Frasi estrapolate dall'intervista a Fabrizio Filippi, Direttore Operativo di Sogemar

Aspetti soft

E' presente nell'azienda un codice di condotta ed una vision aziendale che parte dalla capogruppo.

"Ci crede l'azionista, ci credono gli amministratori delegati dei vari gruppi, ci crede la forza dirigenziale nella politica aziendale e quindi a cascata anche gli operatori." [*]

L'impatto è su tutti i fattori causa interni: *"questo impatta sulla collusione, ma anche sulle procedure, impatta su tutto."* [*]

Continous improvement

L'azienda cerca di coinvolgere i dipendenti per migliorare le procedure organizzando delle riunioni ad-hoc.

"Noi facciamo gruppi, sottogruppi, tiriamo al tavolo chi è attivo sul pezzo e lanciamo dei segnali per far capire cosa bisogna migliorare; per noi la persona è il bene dell'azienda ed è questo il successo dell'azienda, si possono avere le migliori strutture ma sono le persone che fanno la differenza. Anche sotto l'aspetto della sicurezza siamo molto sensibili." [*]

"Da un loro coinvolgimento è venuta fuori una loro idea, abbastanza banale ma molto efficace,cioè quella di attrezzare il carro ferroviario con delle sbarre anti-intrusione così da impedire l'apertura del container se caricato sul carro." [*]

L'impatto è sia sul miglioramento delle procedure che sulla motivazione dei dipendenti e quindi sull'attenzione nello svolgere le procedure.

"E' chiaro che avendole proposte loro e vedendole implementate, si sentono così realizzati da proporre nuove soluzioni e lavorare meglio giorno dopo giorno." [*]

Si ha quindi un impatto interno sia a livello operativo che di miglioramento delle procedure esistenti sia lato attacchi che lato fornitura.

Business continuity planning

Non esiste un action plan prestabilito ma, tramite un sistema di controllo satellitare, l'informazione dell'eventuale disruption viene assimilata immediatamente e questo consente una rapida risposta del management.

"Tutti i nostri il camion sono dotati di sistema satellitare ed esiste un software che viene fatto partire alla mattina alle 7 e si vede in tempo reale la situazione di ogni autista, se è fermo, se è in viaggio, ecc.. Se succede qualche anomalia, l'informazione

[*] Frasi estrapolate dall'intervista a Fabrizio Filippi, Direttore Operativo di Sogemar

arriva subito a noi, parte la segnalazione al cliente e pianifichiamo l'alternativa migliore." *

Segnalare incidenti e debolezze

Non esiste un meccanismo formale per accogliere le segnalazioni di anomalie e near misses

"Nel perimetro del terminal c'è un controllo del container quando entra in azienda, e un controllo all'uscita; se c'è qualche discrepanza si va ad indagare." *

L'impatto è sul miglioramento delle procedure sia lato attacchi che fornitura.

Knowledge management

Non esiste una meccanismo di condivisione della conoscenza a livello operativo, viene implementato un controllo a livello manageriale sul numero di anomalie avvenute per poi discutere le cause senza però archiviare in modo formale le esperienze.

"Ogni anomalia ha una codifica (blu se dipende dalla direzione operativa, rossa se dipende dalla direzione commerciale, verde se dipende dalla direzione IT, arancione se dipende dalla direzione amministrazione,ecc. Ogni mese si contano il numero di anomalie causate dalle varie direzioni, ovviamente il maggior numero di anomalie fanno capo alla direzione operativa." *

Valutazione della conformità di sicurezza

Sogemar possiede molte certificazioni di sicurezza.

"Noi siamo certificati 9001 e quindi c'è una visita ispettiva ogni 3 mesi, abbiamo la certificazione ambientale e, tramite la nuova società oceanogate, per entrare a far parte del mondo delle imprese ferroviarie dobbiamo avere il certificato di sicurezza da parte dell'agenzia nazionale della sicurezza ferroviaria che è molto molto stringente, specialmente dopo Viareggio". *

Richiede che i suoi fornitori siano certificati e rispondano a determinati requisiti di sicurezza.

"Io affido ad un soggetto terzo un bene mio per cui richiedo che il vettore sia affidabile (c'è una forte attenzione nella scelta dell'autista),che il deposito sia telecamerato e sorvegliato. Inoltre tutti i nostri mezzi sono satellitari." *

Sogemar effettua in prima persone delle ispezioni per controllare di persona lo stato di sicurezza dei sui partner.

* Frasi estrapolate dall'intervista a Fabrizio Filippi, Direttore Operativo di Sogemar

"Abbiamo degli ispettori interni, così chiamati,che fanno dalle due alle tre visite all'anno ai nostri fornitori; da lì vengono redatte le non conformità per quanto riguarda tutti i processi, da come fa la fattura a come riceve la merce. Se il partner dichiara di avere il piazzale satellitato e poi non ce l'ha per noi questa è una grave non conformità". *

Questa attenzione alle conformità sulla sicurezza impatta su tutti i fattori causa, dalla collusione all'inadeguatezza del partner, dal miglioramento delle procedure ad una loro applicazione più attenta a livello operativo, per comprendere anche una maggior visibilità e collaborazione con i partner.

Partnership

Una politica di Sogemar è quella di far largo ricorso alla partnership, sia con le attuali società di trazione sia con i padroncini.

"Sulle imprese ferroviarie ne abbiamo due, uno è socio, l'alto è partner. Questo ancora per poco perché con la nascita di oceanogate ci integreremo verticalmente e faremo anche la trazione in casa. Per quanto riguarda invece i padroncini la nostra politica è quella di fidelizzare assolutamente questo mondo anche con il sistema del franchising contribuendo finanziariamente, noi non vogliamo più il padroncino con 1/2 camion, vogliamo flotte da 30/40 mezzi e alcuni padroncini non ce la fanno ad esporsi finanziariamente così tanto per cui abbiamo dato una mano con le banche. Noi gli diamo una mano, gli diamo il lavoro e loro devono garantirci affidabilità e anche un'immagine, è fondamentale per noi che il cliente finale sia soddisfatto dal padroncino perché è quella la cosa che vede per primo." *

Avendo un rapporto consolidato con i partner si ha un'implementazione migliore delle procedure che un miglioramento delle stesse sia lato attacchi che fornitura. Aumenta inoltre l'adeguatezza del fornitore e la sua collaborazione e la visibilità.

"L'autista per noi è una fonte di informazione, per noi l'autista è un commerciale anche perché se prendiamo noi i viaggi questi passano a lui." *

Anche per quanto riguarda la collusione, questo strumento ha degli impatti.

"Lavorando su strutture consolidate da anni, sapendo la nostra politica, la scelta da parte dei padroncini, degli autisti passa attraverso una selezione molto dura" *

* Frasi estrapolate dall'intervista a Fabrizio Filippi, Direttore Operativo di Sogemar

Sviluppo della consapevolezza sulla sicurezza con i partner

Il processo di sviluppo della consapevolezza sulla sicurezza non viene esteso al di fuori dei confini aziendali infatti*"le riunioni con i partner non vengono effettuate perché diventa difficile, ci limitiamo alle visite ispettive."* [*]

Riduzione della differenza di cultura tra azienda e partner

Non vengono effettuate riunioni o eventi di socializzazione anche se *"ci stiamo riflettendo ma non lo ritengo uno strumento maturo, è uno strumento molto importante per DHL, UPS dove l'operatore entra proprio nel cuore dell'azienda, in ufficio magari durante una riunione."* [*]

Focus sul cliente finale

Non esiste un'incentivo di filiera, per cui è difficile avere una visione che non si limiti ai confini aziendali ma guarda alla prestazione finale per il cliente. Anche se in Sogemar viene considerata importante l'immagine che i padroncini esprimono ai clienti (essendo loro un'estensione dell'azienda) non vengono riconosciuti degli incentivi a meno di casi estemporanei.

"Difficile avere un'integrazione così trasversale, anche perché di difficile misurazione. Ad esempio per i padroncini ogni tanto si lanciano dei segnali: l'anno scorso abbiamo premiato chi aveva il camion tenuto meglio, quest'anno non l'abbiamo riproposto anche perché bisogna fare i conti poi con il budget a disposizione." [*]

Grado di importanza degli strumenti

Sono stati individuati come strumenti più importanti gli strumenti interni, in particolare l'integrità, lealtà tra dipendenti e la collaborazione tra dipendenti.

"Una volta che c'è questo il 90% è fatto perché vuol dire che si è riusciti a trasmettere la filosofia all'intera azienda." [*]

Uno strumento ritenuto importante è il focus sul cliente, anche se non è applicato nella nostra accezione più ampia di incentivo e competizione di filiera e non di singola azienda.*" Un altro fattore molto importante è come si presenta il padroncino dal cliente, l'immagine che da di sé."* [*]

[*] Frasi estrapolate dall'intervista a Fabrizio Filippi, Direttore Operativo di Sogemar

Peso dei fattori causa

Per quanto riguarda il KPI Furti/manipolazioni, la causa più frequente risulta essere l'inadeguatezza delle procedure, seguita dalla errata/mancata implementazione e in ultima la collusione.

"Sono i fattori esterni che causano i furti; ci sono squadre specializzate che vanno oltre le procedure; mentre la collusione non l'abbiamo mai riscontrata." [*]

Lato Fornitura invece la causa principale che provoca ritardi è da imputare ad incomprensioni e quindi ad una comunicazione sbagliata o mancata.

"E' un mix di tutte le cose, forse la causa principale non è la mancata collaborazione ma la presenza di incomprensioni." [*]

Di seguito è riportata la tabella compilata durante l'intervista.

[*] Frasi estrapolate dall'intervista a Fabrizio Filippi, Direttore Operativo di Sogemar

		SICUREZZA DA ATTACCHI			SICUREZZA DI FORNITURA			
		1	2	3	4	2	2	2
	Lo strumento viene utilizzato in azienda?	Collusione	Errata/mancata implementazione delle procedure	Inadeguatezza delle procedure	Mancata collaborazione / visibilità con i partner	Inadeguatezza partner	Errata/mancata implementazione delle politiche gestionali	Inadeguatezza delle politiche gestionali
Forza lavoro multidisciplinare	**f.**		↓				↓	
Collaborazione tra dipendenti	**f.**		↓				↓	
Integrità, lealtà dei dipendenti	**f.**	↓	↓				↓	
Sviluppo della consapevolezza interna sulla sicurezza	**f.**		↓				↓	
Aspetti soft	**f.**	↓	↓	↓			↓	↓
Continuous improvement	**f.**		↓	↓			↓	↓
Business continuity planning	**NO**							
Segnalare incidenti e debolezze	**n.f.**			↓				↓
Knowledge management	**NO**							
Valutazione della conformità di sicurezza	**f.**	↓	↓	↓	↓	↓	↓	↓
Partnership	**f.**	↓	↓	↓	↓	↓	↓	↓
Sviluppo della consapevolezza sulla sicurezza con i miei partner	**NO**							
Riduzione della differenza di cultura tra aziende e partner	**NO**							
Focus sul cliente	**NO**							

Evidenziati in giallo gli strumenti ritenuti indispensabili per ottenere performance sicure e i principali fattori che causano una minore sicurezza da attacchi e fornitura, la scala utilizzata per i fattori causa è in ordine crescente di importanza.

La risposta "n.f." sull'utilizzo dello strumento in azienda significa che lo strumento viene utilizzato in azienda ma non in maniera standard o formale.

D.11 T.IMO.

Tipologia azienda: terminal intermodale

Area di responsabilità diretta: cambio di modalità di trasporto

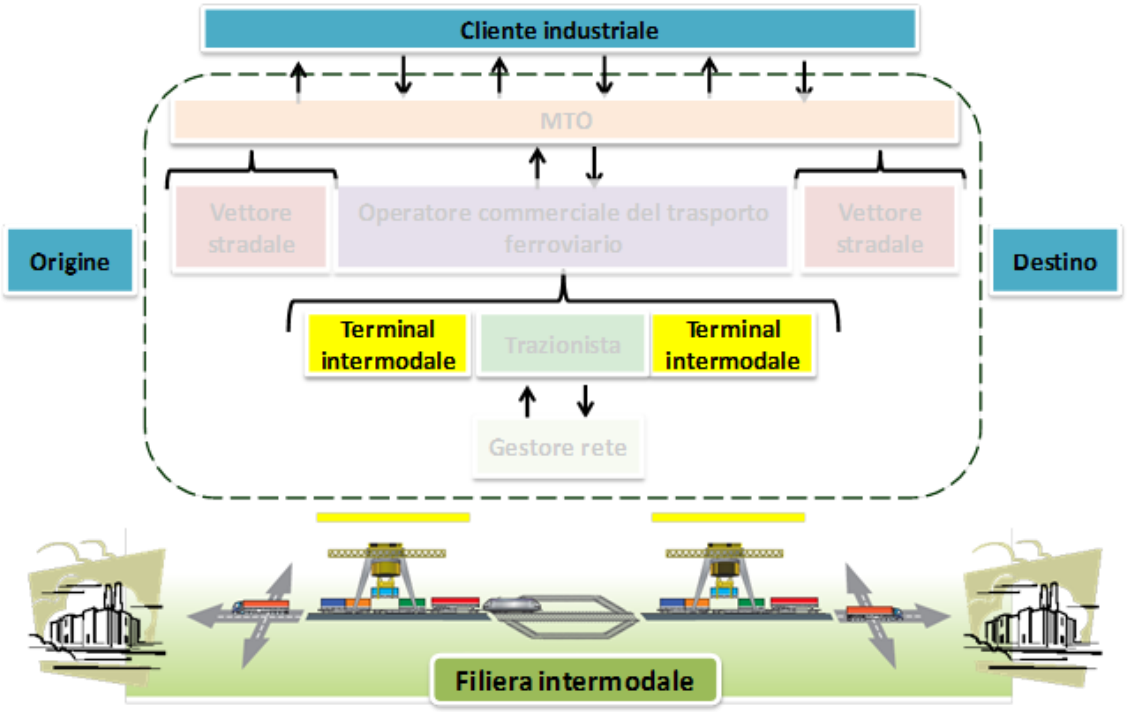
Proprietà: controllata al 71% da Polo Logistico Integrato di Mortara, al 15% da Argo Finanziaria e al 14 % da Den Hartogh.

Fatturato: 414864€ (2010); 700.000-750.000€ (previsioni per il 2011)

Dipendenti: 4 interni + 4 esterni

Interlocutore: Ing. Davide Muzio, Consigliere Delegato

Sede intervista: Uffici c/o Terminal Intermodale di Mortara (PV)



Premessa

"T.I.MO. srl" ovvero "Terminal Intermodale di Mortara srl" è la società di gestione dell'impianto intermodale di Mortara. Costituita il 6 giugno 2008, la Società si propone di promuovere il trasporto ferroviario delle merci attraverso lo scambio gomma-ferro.
Socio di maggioranza in TIMO è la Polo Logistico Integrato di Mortara. Gli altri Soci sono l'olandese Den Hartogh, operatore logistico specializzato nella filiera industriale chimica e Argo Finanziaria, società operante nel settore autostradale, trasporto merci e logistica. Tutti i soci contribuiscono ad apportare le proprie esperienze e traffici al terminal che ha il carattere di impianto aperto al pubblico.
TIMO è inserito all'interno del Parco Logistico Intermodale di Mortara, in un contesto particolarmente ricco di infrastrutture, tale da garantire una capillare ed efficiente rete di trasporto per le merci che transitano dal terminal verso l'Italia e l'estero. È localizzato in una posizione strategica, all'incrocio tra il Corridoio trans-europeo n°5 (Lisbona-Kiev) e il corridoio n° 24 (Genova-Rotterdam), e collegato col sistema portuale ligure, con i valichi transalpini, con l'alea metropolitana milanese e con la rete stradale primaria.
Il Terminal Intermodale di Mortara è un terminal di medie dimensioni, inaugurato nel 2009, e che attualmente gestisce il traffico di treni shuttle su Rotterdam assieme ad un operatore olandese.
Il terminal si estende su un'area di oltre 100.000 m² ed è caratterizzato da un modulo intermodale di tre binari operativi per il carico/scarico, predisposti e pensati in ottica di utilizzo di gru a portale, e da un fascio di 4 binari elettrificati per la presa/consegna dai treni. Gli arrivi e le partenze dei convogli sono direttamente possibili dal terminal, comportando benefici economici e di tempo nella gestione delle manovre e nelle procedure tecnico-amministrative. Annesse al terminal, sono previste aree logistiche per circa 340.000 mq di cui circa 180.000 coperti destinati a magazzini.
Dal punto di vista operativo, TIMO gestisce le operazioni di handling di ILU attraverso gru semoventi, con la possibilità di potere utilizzare in un futuro gru elettriche a portale su rotaie quando ci saranno flussi maggiori. La capacità massima di progetto prevede fino a 9 coppie di treni giornalieri con una stima di traffico di 150.000 ILU annui a regime. Attualmente vengono fatte 5 coppie alla settimana sul corridoio Genova-Rotterdam.

Dal punto di vista della filiera, TIMO si interfaccia con l'MTO, che è il suo unico vero cliente, con l'azienda di trasporto su gomma che ritira/consegna le ILU del cliente finale e infine con il trasportatore ferroviario che esegue le manovre di ingresso e uscita dal terminal dei treni. Azienda di trasporto e trasportatore ferroviario sono rispettivamente cliente e fornitore dell'MTO.

TIMO ha un campo di responsabilità limitato alle sole attività di handling delle ILU. Il terminal riceve i container già caricati e sigillati assieme a una bolla che ne dichiara il contenuto, e una volta finito il carico del treno li consegna al vettore ferroviario. Una eventuale difformità tra quanto dichiarato e il contenuto effettivo è di responsabilità del dichiarante ovvero del trasportatore.

Il contributo di Davide Muzio offre non solo un punto di vista sull'operato di un terminal intermodale giovane e in crescita che ha problematiche e responsabilità quasi esclusivamente legate all'operatività, ma anche una visione più ampia, derivante da anni di esperienza in realtà ben più complesse. La sua carica per anni di *Direttore della produzione e logistica* di uno dei più grossi operatori intermodali della realtà italiana e europea, ha reso possibile la trattazione degli argomenti con uno sguardo comparativo tra le diverse realtà e con una sensibilità ancor maggiore nella trattazione di problematiche sulla sicurezza da attacchi e di fenomeni collusivi.

Adozione degli strumenti

Forza lavoro multidisciplinare

In TIMO non si può parlare di un vera e propria forza lavoro organizzata in team, solamente perché si tratta di un'azienda per il momento piccola con pochi dipendenti. Il nostro interlocutore non esclude che al crescere della numerosità dei dipendenti si possa adottare un'organizzazione in team formale.

"Facciamo 5 coppie d treni alla settimana e al momento quindi non abbiamo una forza lavoro tale da richiedere un'organizzazione in team. È chiaro che c'è un'organizzazione con dei ruoli, ma piuttosto semplice. C'è un capo terminal che gestisce 2 figure ti tipo impiegatizio-operativo e le persone esterne che eseguono operazioni di gruaggio. Gli operatori del trasporto ferroviario per le manovre non dipendono da noi, ma ricevono le indicazioni direttamente da noi".[*]

[*] Frasi estrapolate dall'intervista a Davide Muzio, Consigliere Delegato di T.I.MO

Tuttavia, sia nei terminal piccoli che in quelli più complessi, è buona norma che un operatore sia multi-tasking, non tanto per motivi di sicurezza, ma per essere operativamente flessibili.

"Proprio perché siamo in pochi dobbiamo saper far più cose. In un terminal, grande o piccolo che sia, trattando una serie di operazioni, tutti devono sapere cosa avviene prima e cosa dopo ed avere perciò una competenza allargata.

Sicuramente la multidisciplinarità abbassa gli errori nelle procedure. Ad esempio, se chi lavora al check-in riceve un'unità e si accorge che c'è qualcosa che non va, può fermare subito l'unità e risolvere il problema in 5 minuti assieme all'autista. D'altra parte se al check-in non ci si accorge che l'unità ha un problema, l'unità procede nel terminal e a quel punto i tempi e i costi per la risoluzione del problema aumentano. C'è una curva dei costi di intervento parabolica tale che prima si interviene meglio è". *

Collaborazione tra dipendenti

Come già detto sopra, non esiste un'organizzazione formale in team, per cui la collaborazione si manifesta in modo informale per esigenze

Lo stesso esempio sulla multidisciplinarità può essere inteso anche in termini di collaborazione tra dipendenti, la quale comporta sicuramente effetti positivi sull'esecuzione delle procedure, sia lato fornitura che attacchi. Inoltre, lavorando a stretto contatto con altre persone, diminuisce la probabilità di collusione.

"Secondo la mia esperienza, gli episodi di collusione raramente coinvolgono la pluralità delle persone. È quasi sempre un singolo che mette in atto qualcosa di collusivo con attori esterni perché c'è un rischio nel condividere un atto criminoso tra colleghi. Il fatto che su un singolo task ci siano più persone che lavorano contemporaneamente può sicuramente diminuire il rischio che ci sia un evento collusivo tipo furto o rapina". *

Integrità, lealtà dei dipendenti

TIMO è sicuramente un'azienda più orientata all'operatività che agli aspetti culturali, per cui non vengono messe in atto politiche formali per favorire la diffusione di valori sulla sicurezza e lealtà dei dipendenti.

A livello informale, l'azienda comunica l'importanza di un comportamento leale e responsabile volto a massimizzare il risultato del gruppo più che del singolo.

* Frasi estrapolate dall'intervista a Davide Muzio, Consigliere Delegato di T.I.MO

Vengono pertanto disincentivati comportamenti collusivi o la non comunicazione di errori commessi durante le procedure, evitando allo stesso tempo punizioni eccessive per non favorire l'omertà.

"Spesso un problema, soprattutto se chi lo deve segnalare è la causa del problema stesso, non viene segnalato. In qualche modo si tratta di incentivare o comunicare il fatto che si preferisce di gran lunga che il soggetto dica subito che ha sbagliato anziché aspettare che sia l'azienda a scoprirlo da sola, con risvolti più negativi. Un atteggiamento eccessivamente punitivo incentiva spesso il silenzio in quanto, in questo caso, è percepito come massimizzante l'utilità del soggetto a discapito di quella dell'azienda".[*]

Sviluppo della consapevolezza interna sulla sicurezza

Non vengono fatti corsi ai dipendenti in termini di sicurezza, bensì in termini di safety. In TIMO non esiste una figura responsabile della sicurezza, ma si avvale di consulenti esterni per le problematiche di safety.

L'adozione di corsi sulla sicurezza, per esperienza del nostro interlocutore, dipende dal grado di complessità e dalla dimensione del personale dell'azienda. In una realtà piccola come TIMO è sufficiente la sola esecuzione corretta delle procedure per ottenere un eccellente livello di sicurezza e di servizio; in realtà più grandi e complesse, i corsi per lo sviluppo della consapevolezza sulla sicurezza sono un presupposto per la corretta applicazione delle procedure, che altrimenti verrebbero percepite solo come un peso e non come il mezzo per il perseguimento di obiettivi di sicurezza.

"In termini di sicurezza non facciamo dei corsi perche abbiamo delle procedure che riteniamo essere in linea con i più alti standard qualitativi. Quindi più che altro c'è una spiegazione delle procedure, interiorizzazione e richiamo al rispetto delle stesse.

Essendo piccoli è facile, perché si tratta di istruire poche persone, che oltretutto sono sempre controllate da un supervisore. La sicurezza è un aspetto più delicato nelle organizzazioni più complesse, dove le procedure sono viste talvolta come un rallentamento". [*]

Presupposto fondamentale per il successo di una politica come quella di TIMO, focalizzata sull'esecuzione operativa, è che le procedure siano corrette, snelle e efficaci, ma anche che alla base ci sia un efficace sistema di sicurezza fisico.

[*] Frasi estrapolate dall'intervista a Davide Muzio, Consigliere Delegato di T.I.MO

"Il nostro è un terminal ancora in fase di crescita, ma in sicurezza spendiamo tanto perché abbiamo ad oggi un sistema di antintrusione tra i più moderni che ci siano in campo terminalistico. Tale sistema ha anche scopo preventivo in quanto funge da deterrente. Fino ad oggi non si è verificato ancora nessun furto".[*]

Aspetti soft

Come abbiamo già detto, TIMO è poco focalizzata sugli aspetti culturali trattandosi di un'azienda di piccole dimensioni.

"Non abbiamo nessuno slogan perché in questo momento non è qualcosa di essenziale. Il messaggio che vogliamo trasmettere è quello per cui si vuole offrire un servizio eccellente".[*]

La scarsa numerosità del personale le permette di tenere sotto controllo l'operato di tutti, e quindi è sufficiente avere delle procedure "ben fatte" per ottenere ottime prestazioni di sicurezza e servizio.

Continous improvement

In TIMO è ben visto un coinvolgimento degli operatori nella revisione e miglioramento delle procedure, ma la scarsa numerosità del personale non dà adito a un processo formalizzato. Inoltre coinvolge anche gli attori esterni all'azienda, ma che operano all'interno delle procedure.

"Siamo in pochi, quindi non è necessario avere un sistema strutturato di raccolta informazione e opinioni. Per il miglioramento continuo abbiamo sia flussi di informazione tipo bottom-up che top-down, oltre a incontri periodici con il personale per evidenziare eventuali criticità.

Sicuramente dove le nostre procedure coinvolgono esterni si cerca di ottenere suggerimenti anche da parte loro". [*]

Per quanto riguarda gli impatti che si possono ottenere, essi sono positivi sia per quanto riguarda l'errata/mancata implementazione delle procedure sia per la loro eventuale necessità di miglioramento.

"A volte una procedura c'è ma non viene eseguita correttamente. In certi casi basterebbe fare una check-list di spunta per implementarla correttamente".[*]

[*] Frasi estrapolate dall'intervista a Davide Muzio, Consigliere Delegato di T.I.MO

Business continuity planning

TIMO, come la maggior parte delle aziende del settore, non può fare affidamento a un action plan esaustivo a causa del gran numero di variabili in gioco.

"Ci sono piani prestabiliti in termini di safety, soprattutto se in incidenti sono coinvolti materiali pericolosi.

*In termini di furto o rapina è più difficile. Non si hanno piani di reazione perché la casistica è molto ampia. In un furto con destrezza magari ci si accorge dopo giorni, in una rapina a mano armata si chiamano subito le forze dell'ordine o magari sono intervenute già prima perché avvisate dal nostro sistema di sorveglianza". **

Non ha molto senso parlare di action plan anche nel caso di ritardi, perché dipende dall'entità del ritardo e dalle risorse disponibili al momento.

Le azioni da mettere in pratica si decidono al momento, e a tal proposito il nostro interlocutore ci fa notare che in una realtà così piccola è più semplice gestire le emergenze rispetto alle realtà complesse che hanno più variabili di decisione.

"Un terminal grande, che gestisce una flotta di carri propri, può decidere, se il treno è in ritardo, di usarne un altro per fare il treno in partenza, di spostare risorse da un settore all'altro, di ripianificare sequenze di carico scarico, oppure in ultima analisi decidere se sopprimerlo o meno.

*I gradi libertà per noi sono inferiori, per cui certe azioni sono obbligate. Per noi che siamo un terminal semplice, se il treno è in ritardo noi non possiamo fare altro che aspettarlo o cancellare la partenza corrispondente. Se i treni arrivano alla sera per la partenza nella stessa serata si tratta solo di decidere se ciò sia fattibile o meno in base alle risorse disponibili. Eventualmente si può decidere di effettuare straordinari".**

Segnalare incidenti e debolezze

Come già anticipato parlando di integrità e lealtà dei dipendenti, TIMO incentiva i dipendenti a mantenere comportamenti volti all'interesse comune, per cui è fortemente consigliato segnalare sempre qualsiasi anomalia, anche da parte di chi non esegue il controllo. La multidisciplinarietà, come già visto, fa si che tutti gli operatori conoscano bene tutto il processo e anche il lavoro degli altri.

*"Ad esempio chi sta facendo il controllo del carico si accorge che c'è un carro con problema lo segnala all'impresa ferroviaria ed evita di caricare il carro". **

* Frasi estrapolate dall'intervista a Davide Muzio, Consigliere Delegato di T.I.MO

I benefici in questo caso si ottengono anche a livello di filiera perché permette di contenere le inefficienze operative che si susseguirebbero nel caso non si contenesse fin da principio l'anomalia. (Riferimento alla curva dei costi di intervento).

Per quanto riguarda la segnalazione dei near messes, il nostro interlocutore ne condivide l'importanza, e a suo parere può essere vista insieme al miglioramento continuo. Gli impatti che si ottengono sono gli stessi.

" Nel momento in cui succede qualcosa, facciamo in modo che non succeda più; se stava per succedere mettiamo le condizioni affinché non succeda". *

Knowledge management

Data la dimensione e il focus prettamente operativo dell'azienda, non è presente un sistema di gestione della conoscenza.

Secondo l'esperienza del nostro interlocutore, anche nelle aziende più complesse del settore è poco usato. A suo parere, questo perché non viene percepito necessario.

"In generale si parte da una procedura ritenuta corretta. Al verificarsi di una anomalia non precedentemente contemplata si tratta di decidere se e come colmare il gap. Una alternativa è sempre non colmare il gap e accettare il rischio eventualmente agendo diversamente ad esempio con coperture assicurative. Una volta colmato l'eventuale gap si ritorna al punto di partenza con la nuova procedura corretta, fino all'eventuale ulteriore anomalia. Solo le organizzazioni più evolute hanno delle figure preposte alla revisione critica delle procedure a priori, anche attraverso una sorta di stress test". *

Valutazione della conformità di sicurezza

TIMO lavora con attori, quali vigilanza e fornitori, che possiedono una serie di certificazioni, per cui si suppone non serva un'ulteriore valutazione della conformità. Per quanto riguardano i clienti, in linea teorica non ci sarebbe nemmeno bisogno di certificazioni o eventuali indicatori di qualità.

"Non ha senso dal lato della sicurezza da attacchi perché non si possono chiedere certificazioni che dicono che il fornitore o il cliente non è un criminale". *

Dal lato fornitura, invece, possono esserci problemi tra MTO e operatore ferroviario relativamente ai ritardi, a tal scopo esistono infatti dei contratti di qualità. Sui i terminal, invece, ci viene detto che in generale non esistono contratti di qualità.

* Frasi estrapolate dall'intervista a Davide Muzio, Consigliere Delegato di T.I.MO

*"I maggiori operatori intermodali spesso non riconoscono contratti sulla qualità verso i loro clienti. Ad esempio se il cliente non consegna delle unità precedentemente prenotate non scatta nessuna penalizzazione. A questo problema si cerca di ovviare però con altre forme contrattuali, con sconti ad esempio, al fine di incentivare comportamenti virtuosi. Viceversa disservizi arrecati da parte dell'operatore intermodale possono dare origine a contenziosi che spesso si risolvono con soluzioni di tipo commerciale". **

Per questo motivo abbiamo riscontrato un utilizzo non formale dello strumento, con impatto positivo sull'errata/mancata implementazione lato fornitura dal punto di vista esterno.

Partnership

TIMO, data la sua recente nascita, non ha avuto la possibilità di poter instaurare un vero e proprio rapporto di lungo periodo.

Sviluppo della consapevolezza sulla sicurezza con i partner

TIMO non si impegna in prima persona nella formazione e training degli operatori esterni, ma impone a loro, dove sono coinvolti, le proprie procedure perché considerate idonee e sicure.

TIMO detta quindi il modo di operare, ma non si pone come l'attore della filiera responsabile della divulgazione e formazione continua sulle pratiche operative e di sicurezza.

Riduzione della differenza di cultura tra azienda e partner

Con partner intendiamo l'MTO in senso lato, in quanto TIMO si interfaccia con i suoi clienti e fornitori. L'azienda non implementa in prima persona questo strumento ma è coinvolta dai suoi partner di filiera.

*"Abbiamo delle procedure messe in atto con la ferrovia e con i padroncini, che comportano una serie di scambi informali e di relazioni proprio tese per minimizzare problemi di qualsiasi tipo. Entrambi devono raggiungere un certo obiettivo minimizzando costi diretti e indiretti e noi abbiamo lo stesso interesse ad arrivare nella stessa direzione". **

* Frasi estrapolate dall'intervista a Davide Muzio, Consigliere Delegato di T.I.MO

Focus sul cliente finale

TIMO dichiara di avere un forte focus sul cliente, non strettamente inteso come il cliente proprio, ossia l'MTO, ma in senso esteso anche ai clienti del cliente.

"Nel terminal non vengono mai i disponenti, ma gli autisti che erroneamente possono essere considerati come ininfluenti; invece loro sono i veri clienti perché sono portatori della qualità percepita del servizio e sono in grado di influenzare la scelta di un terminal piuttosto che l'altro. L'attenzione alla parte terminale del cliente, che in questo caso è l'autista, è fondamentale perché sulla base della soddisfazione del cliente finale ci si gioca una buona reputazione o meno presso l'organizzazione cliente". *

L'argomentazione del nostro interlocutore dimostra che il loro obiettivo ultimo non è solo quello di soddisfare il cliente diretto (MTO), ma è di loro interesse soddisfare tutti gli attori della catena logistica di riferimento al fine di instaurare rapporti di collaborazione e per consolidare relazioni di lungo periodo.

Tuttavia una relazione caratterizzata da eccessiva fiducia e familiarità potrebbe impattare in modo negativo, perché dal punto di vista delle procedure, potrebbe generare errori e omissioni. Ad esempio una procedura che prevedesse autorizzazioni formali potrebbe essere by-passata in fiducia, con pericolose conseguenze nel seguito in tema di responsabilità.

"Dove c'è un'eccesiva prossimità tra autisti e personale interno, si possono instaurare più facilmente comportamenti collusivi. Bisogna offrire un buon servizio senza eccedere in familiarità". *

Grado di importanza degli strumenti

Tra gli strumenti analizzati quello ritenuto indispensabile per ottenere performance sicure è stato individuato anzitutto nella collaborazione dei dipendenti.

"La collaborazione tra i dipendenti va intesa sia in senso orizzontale che verticale. Nel senso orizzontale è molto facile che tra persone che devono fare lo stesso mestiere ci si scambi informazioni per farlo meglio. Se ci si limitasse a questo, tale know how rimarrebbe circoscritto e poco strutturato. La collaborazione verticale fa sì che eventuali proposte migliorative siano valutate in termini di vantaggi e svantaggi e possano essere eventualmente tradotte in procedure diventando di fatto know how aziendale". *

* Frasi estrapolate dall'intervista a Davide Muzio, Consigliere Delegato di T.I.MO

La collaborazione su questo secondo asse noi l'abbiamo intesa come continuous improvement, che difatti viene applicato in azienda seppur in modo informale.
La comunicazione interna spinge principalmente sul concetto di interesse comune e quindi a segnalare gli incidenti e debolezze da una parte e suggerimenti migliorativi dall'altra.

Peso dei fattori causa

Per quanto riguarda la sicurezza da attacchi, che si traduce unicamente nei tentativi di furti e rapine nel terminal, fino ad oggi non è ancora stata messa alla prova perché non si sono verificati furti o rapine. Secondo il nostro interlocutore, che possiede una vasta conoscenza sull'argomento, le principali cause di furti sono da attribuire, in ordine di importanza, all'errata/mancata implementazione delle procedure e infine alla collusione.
Per quanto riguarda la sicurezza di fornitura, l'inadeguatezza del partner è stata individuata come la prima causa dei ritardi provocati nella filiera, con un'incidenza qualitativa del 60% sulla prestazione. Segue la mancata collaborazione e visibilità con i partner con un'incidenza del 35%.
"Se il fornitore è in ritardo e lo sappiamo all'ultimo, non possiamo in alcun modo contenere il ritardo. Se invece lo veniamo a sapere in anticipo, grazie all'elevata flessibilità e al focus sul cliente, riusciamo a ripianificare il lavoro minimizzando il danno". [*]
Hanno un ruolo marginale invece sulla prestazione di sicurezza di fornitura l'errata / mancata implementazione delle procedure e l'inadeguatezza delle stesse, che insieme raggiungono a malapena il 5% di incidenza sulla sicurezza.

Di seguito è riportata la tabella compilata durante l'intervista.

[*] Frasi estrapolate dall'intervista a Davide Muzio, Consigliere Delegato di T.I.MO

		SICUREZZA DA ATTACCHI			SICUREZZA DI FORNITURA			
		1	3	2	3	4	2	2
	Lo strumento viene utilizzato in azienda?	Collusione	Errata/mancata implementazione delle procedure	Inadeguatezza delle procedure	Mancata collaborazione / visibilità con i partner	Inadeguatezza partner	Errata/mancata implementazione delle politiche gestionali	Inadeguatezza delle politiche gestionali
Forza lavoro multidisciplinare	**n.f.**		↓				↓	
Collaborazione tra dipendenti	**n.f.**	↓	↓				↓	
Integrità, lealtà dei dipendenti	**n.f.**	↓	↓				↓	
Sviluppo della consapevolezza interna sulla sicurezza	**NO**							
Aspetti soft	**NO**							
Continuous improvement	**n.f.**		↓	↓			↓	↓
Business continuity planning	**NO**							
Segnalare incidenti e debolezze	**n.f.**		↓	↓			↓	↓
Knowledge management	**NO**							
Valutazione della conformità di sicurezza	**n.f.**						↓	
Partnership								
Sviluppo della consapevolezza sulla sicurezza con i miei partner	**n.f.**					↓		
Riduzione della differenza di cultura tra aziende e partner	**NO**							
Focus sul cliente	**NO**							

Evidenziati in giallo gli strumenti ritenuti indispensabili per ottenere performance sicure e i principali fattori che causano una minore sicurezza da attacchi e fornitura, la scala utilizzata per i fattori causa è in ordine crescente di importanza.

La risposta "n.f." sull'utilizzo dello strumento in azienda significa che lo strumento viene utilizzato in azienda ma non in maniera standard o formale.

D.12 Terminali Italia

Tipologia azienda: terminal intermodale puro

Area di responsabilità diretta: cambio di modalità di trasporto

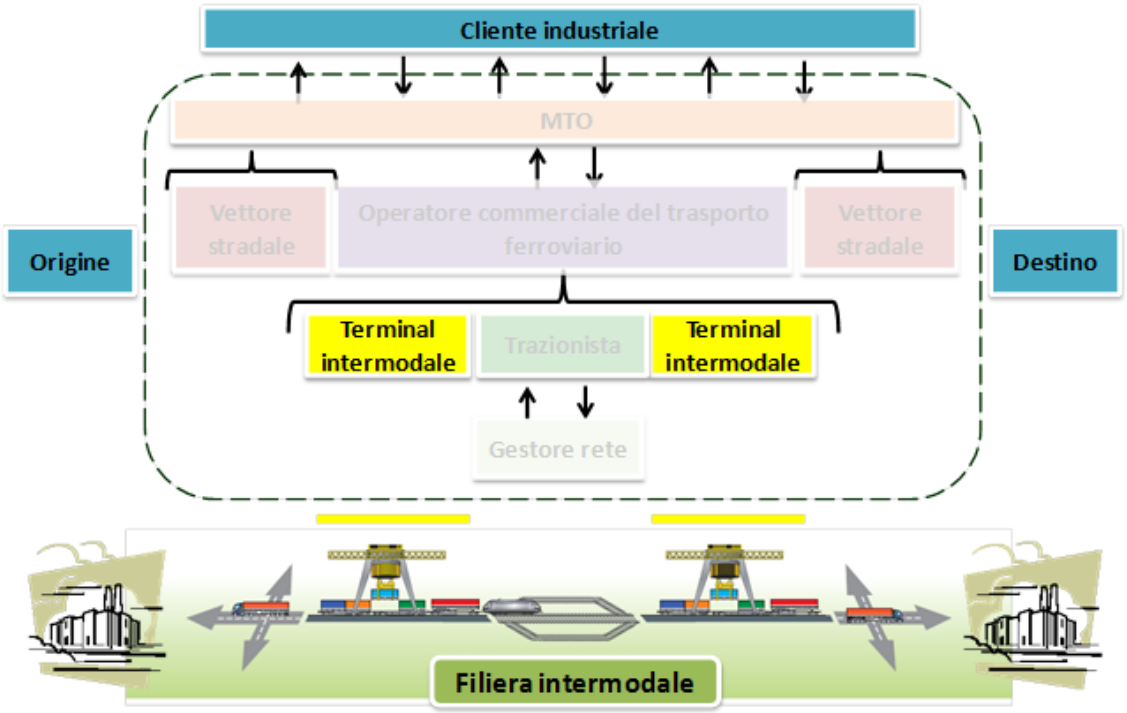
Proprietà: controllata all'89% da RFI (Rete Ferroviaria Italiana) e dall'11% da CEMAT

Fatturato: 16,5 mln € (2009)

Dipendenti: 202

Interlocutore: Aldo Locurcio, Responsabile del centro intermodale di Segrate (MI)

Sede intervista: Uffici di Terminali Italia presso il terminal di Segrate (MI)



Premessa

Terminali Italia è la società del gruppo Ferrovie dello Stato che si occupa della gestione integrata dei servizi terminalistici all'interno del network dei terminali intermodali di RFI.

Di responsabilità di Terminali Italia è la gestione dei servizi connessi all'ultimo miglio ferroviario (handling e manovra).

Il network di Terminali Italia è esteso a tutto il territorio italiano e conta oggi 20 terminal intermodali con sede a Bari, Brescia, Bologna, Castelguefo, Catania, Livorno, Gela, Marcianise, Pescara, Roma, Torino, Verona, Villaselva, più due terminal a Brindisi e Padova, e tre terminal a Milano (Certosa, Segrate e Smistamento).

La nostra intervista si è concentrata sull'operato del terminal di Segrate (MI), un centro intermodale di medie dimensioni che possiede l'intero personale dipendente dislocato tra gli uffici e il piazzale dove operativamente si svolge il cambio di modalità di trasporto.

Il terminal ha una capacità di movimentazione di circa 90.000 TEU e da due anni è di proprietà di RFI, mentre precedentemente era posseduto da CEMAT.

Il terminal possiede otto binari per la traslazione (trasbordo di un container dal vettore stradale a quello ferroviario e viceversa) e offre un servizio intermodale puro, senza funzioni annesse di deposito logistico. Lavora sul territorio nazionale, con direttrici verso il nord-est Italia e il sud Italia, e su quello internazionale con direttrici principali Belgio e Germania.

Il processo di spedizione è così strutturato : gli operatori di trasporto multimodale (MTO o operatori commerciali del trasporto ferroviario) devono effettuare la prenotazione di carico sul sistema SAP del terminal, una volta confermato l'appuntamento il mezzo in arrivo al terminal svolge l'accettazione per poi essere destinato al binario di partenza associato. A questo punto gli operatori comunicano la lista di carico del treno, così che al terminal si possa effettuare il corretto trasbordo dei contenitori e il trasporto al nastro arrivi e partenze. Il treno può quindi essere rilasciato all'impresa ferroviaria che prima della partenza si occuperà della verifica tecnica delle unità e della preparazione dei documenti per il trasporto.

È compito degli operatori del terminal controllare l'integrità dei contenitori in partenza e in arrivo (sigilli, anomalie, ammaccature), controllo che poi verrà anche effettuato dall'operatore ferroviario alla partenza e all'arrivo del treno.

Il terminal si interfaccia dunque sia con gli operatori commerciali del trasporto ferroviario, sia con gli operatori ferroviari ma limita la sua area di responsabilità al solo terminal e al solo processo di carico/scarico dei contenitori, senza avere visibilità sull'interezza del traposto da fornitore a cliente.

Il centro intermodale ha quindi una responsabilità molto limitata nel processo di trasporto, e anche le problematiche che deve affrontare sono piuttosto circoscritte; per quanto riguarda le minacce intenzionali le uniche reali problematiche sono i tentativi di furti ai contenitori stivati nel piazzale in attesa di essere caricati, o appena scaricati e in attesa di essere trasportati al cliente finale. Le minacce di manipolazione della merce, o tentativi di trasporti non autorizzati solitamente si verificano nelle soste del treno durante il tragitto ferroviario, e quindi non rientrano nelle responsabilità del terminal, che si limita alla verifica dei sigilli e dei dispositivi di sicurezza sui contenitori, per eventualmente fare riserve sul trasporto e aspettare l'intervento di un perito. Per aumentare la sicurezza, i contenitori a terra vengono stivati porta contro porta, e durante la notte è presente un servizio di vigilanza della polizia ferroviaria.

Per quanto riguarda la sicurezza di fornitura invece gli imprevisti possono essere operativi o gestionali, con frequenza di accadimento molto maggiore rispetto agli attacchi intenzionali.

Il contributo di Aldo Locurcio offre un punto di vista sull'operato di un terminal intermodale che ha problematiche e responsabilità quasi esclusivamente legate all'operatività, e nel quale l'aspetto di gestione delle risorse umane e di cultura della sicurezza ha decisamente una minore rilevanza.

Adozione degli strumenti

Forza lavoro multidisciplinare

La formazione e le competenze tecniche degli operatori sono legate strettamente al compito che devono svolgere con focus sulle procedure da seguire.

"La formazione che riceve l'operaio è esclusivamente legata alla sua mansione. In aggiunta gli facciamo svolgere i corsi di formazione per pronto soccorso, pratiche antincendio e per la movimentazione di merce pericolosa (ADR). C'è da dire che la formazione teorica non è la componente principale ma è molto più importante l'esperienza sul campo che consente di imparare effettivamente il lavoro". [*]

[*] Frasi estrapolate dell'intervista ad Aldo Locurcio, responsabile del terminal intermodale di Segrate

È evidente, quindi, come per la formazione degli operatori il learn by doing sia più importante della formazione strettamente teorica. Inoltre l'azienda ritiene che sia più utile avere una forza lavoro specializzata piuttosto che con competenze diffuse.
Un altro aspetto legato alle competenze e alle informazioni che ricevono gli operatori, è la possibile relazione con la collusione.
"Il nostro è un lavoro particolare in cui ogni giorno ci passa sotto gli occhi diversa tipologia di merce. Difatti la procedura di accettazione viene svolta dagli impiegati e all'operatore (gruista) viene comunicata solo la destinazione del container per il corretto posizionamento nell'area preposta (piazzale).
Nel caso di container spiombati, gli impiegati che eseguono le spunte dei treni in arrivo sanno applicare la procedura del caso (messa in sicurezza dell'unità, procedura in essere per avvisare l'MTO e il cliente)".[*]
Il tema del controllo e della diffusione delle informazioni, è quindi ritenuto un altro aspetto importante dal nostro interlocutore.

Collaborazione tra dipendenti

La collaborazione tra dipendenti e il lavoro in team non sono elementi ricercati volontariamente ma in ogni caso si verificano essendo le stesse mansioni che portano gli operatori a lavorare a stretto contatto.
Diversa è invece la situazione per i nuovi assunti che vengono affiancati da personale con più esperienza per poter imparare il lavoro.
"E' impensabile che un nuovo arrivato possa lavorare da solo. Sarebbe rischioso sia per lui che per gli altri. Diciamo che all'inizio la collaborazione e il lavoro in team sono necessari per i nuovi arrivati, ma poi col tempo ognuno si specializza nella sua mansione e sulle proprie responsabilità e il team diventa più una conseguenza del lavoro piuttosto che un elemento progettato". [*]
Pur non essendo ricercata, la collaborazione è stata ritenuta importante per ottenere delle buone performance operative con impatto sia sulla sicurezza da attacchi che su quella di fornitura.

Integrità, lealtà dei dipendenti

Terminali Italia non attua delle politiche per premiare la fedeltà e l'integrità dei dipendenti.

[*] Frasi estrapolate dell'intervista ad Aldo Locurcio, responsabile del terminal intermodale di Segrate

Ragionando in termini teorici però, secondo il nostro interlocutore, un equo sistema d'incentivazione, che tenga conto anche della qualità di lavoro delle persone, potrebbe motivare i dipendenti al meglio.

È ovvio che per Terminali Italia (e nello specifico il terminal di Segrate), facendo parte di un grande gruppo, è più difficile riuscire ad implementare un sistema globale per il controllo e la valutazione del personale.

"Penso che per un'azienda medio/piccola sia più facile fare questo tipo di iniziative. Li infatti chi decide, come il direttore del personale o il proprietario stesso, essendo sempre a stretto contatto con gli operai, può anche decidere personalmente di premiare chi lavorava in un certo". *

Sviluppo della consapevolezza interna sulla sicurezza

Il terminal organizza delle riunioni ogni qual volta vi è la presa in carico di nuove tipologie di merce (circa una volta ogni sei mesi) in cui si diffondono agli operatori le tematiche di sicurezza legate alle nuove procedure adatte per le nuove tipologie di merce. Non esiste però un sistema di misurazione o incentivazione/punizione legato alla sicurezza, se non quello delle lettere di richiamo da contratto nazionale.

"Quando dobbiamo lavorare per un nuovo cliente, che tratta merce diversa da quella che noi solitamente trattiamo, si organizzano dei meeting a cui io partecipo in cui vengono spiegate tutte le procedure del caso. Poi organizzo delle riunioni interne in cui si illustrano le nuove procedure legate alle nuove tipologie di merce agli operatori del terminal". *

La formazione impatta sulla migliore implementazione delle procedure, sia lato attacchi che fornitura.

Aspetti soft

Il terminal ha ereditato le modalità di governance di CEMAT che a sua volta le ha ereditate da TRENITALIA quando quest'ultima è diventata sua principale azionista.

La corporate governance comprende quindi un codice etico ispirato a quello delle Ferrovie dello Stato, un modello organizzativo, di gestione e controllo sotto la responsabilità di un organismo di vigilanza esterno, e un sistema di controllo interno per la gestione dei rischi con l'obiettivo di migliorare l'efficacia e l'efficienza aziendale.

In realtà, l'impatto di questi provvedimenti non sembrano aver influenzato la motivazione degli operatori nel lavoro quotidiano.

* Frasi estrapolate dell'intervista ad Aldo Locurcio, responsabile del terminal intermodale di Segrate

*"Quando è avvenuto il cambio di azionariato di CEMAT, passata sotto il controllo di TRENITALIA, noi ne abbiamo ereditato il codice etico. Successivamente, passando sotto TERMINALI ITALIA, abbiamo mantenuto questo codice etico. Quando CEMAT non era sotto il controllo di TRENITALIA non aveva alcun codice etico, ma devo dire che dal punto di vista operativo non si è percepita molto la differenza. In ogni caso ritengo che la presenza di un codice etico rappresenti un valore aggiunto per l'azienda". **

Continous improvement

Come detto precedentemente agli operai viene richiesto esclusivamente di concentrarsi sul proprio lavoro.

In azienda non esiste una politica che incentivi gli operatori a dare suggerimenti per il miglioramento delle procedure.

Business continuity planning

In caso di situazioni impreviste non esistono piani d'azioni prestabiliti, e in ufficio viene stabilita la soluzione migliore real-time.

*"E' difficile che accada qualcosa che ci obblighi a interrompere il lavoro. Abbiamo a disposizione otto macchine e i meccanici direttamente al terminal per qualsiasi evenienza. Sono successi casi particolari in cui abbiamo avuto quattro macchine ferme, ma anche in quei casi il lavoro è proseguito, dando precedenza ai treni più urgenti e cercando di avvisare preventivamente quei clienti che sarebbero andati in ritardo". **

Segnalare incidenti e debolezze

Tutti gli operatori sono istruiti per segnalare anomalie o eventuali problematiche dei container presenti sul piazzale.

La segnalazione viene fatta informalmente direttamente al capo terminal, o in caso di sua assenza al capo ufficio.

*"Tutti gli operatori sanno che appena vedono qualcosa che non va devono immediatamente segnalarlo. Sanno anche che non devono prendere iniziative perché l'intervento sul contenitore è possibile farlo solo dopo mia disposizione, o del capo ufficio".**

Le segnalazioni riguardano i near misses, perché in caso di incidenti lavorando tutti così a stretto contatto non è neanche necessario dover fare una segnalazione.

* Frasi estrapolate dell'intervista ad Aldo Locurcio, responsabile del terminal intermodale di Segrate

"Le segnalazioni più importanti sono quelle che arrivano da chi lavora sulle gru che dall'alto possono vedere cose che sfuggono a chi è sul piazzale. Se il gruista vede per esempio delle anomalie sul tetto di un container in partenza deve subito segnalarle, così che dall'ufficio possiamo subito intervenire".[*]

Gli impatti delle segnalazioni sono indispensabili per poter attivare una serie di procedure che permettono di non causare ritardo nella filiera.

"Per esempio nel caso di un danneggiamento di un contenitore, che può essere stato causato da noi o da chi ce l'ha consegnato, se non viene subito segnalato è un problema, perché il cliente che viene a ritirarlo non può andare in consegna e fa fare un giro a vuoto ai suoi autisti. Invece con la segnalazione immediata io posso subito contattare il perito e farlo venire per capire la tipologia di danno, e avvisare subito il cliente del problema così da poter fissare un nuovo appuntamento per il ritiro della cassa". [*]

Le segnalazioni sono sempre di natura strettamente operativa, relative all'integrità del container.

Knowledge management

Dato il focus prettamente operativo dell'azienda, non è presente un sistema di gestione della conoscenza.

Valutazione della conformità di sicurezza

Il terminal è autorizzato alla movimentazione di merce pericolosa (ADR) ma non al relativo stoccaggio. Quando era sotto il controllo di CEMAT era anche certificato ISO 9001 ed attualmente, dopo il passaggio a RFI, sta aspettando la medesima certificazione.

Le procedure nel frattempo sono rimaste praticamente le stesse.

L'impatto delle certificazioni e dei relativi controlli non porta però nella pratica ad un effettivo aumento della sicurezza.

"Noi continuiamo a lavorare come se avessimo la certificazione perché fa parte del nostro background, della nostra esperienza. Dopo anni in cui eravamo abituati a lavorare in un certo modo (tramite le procedure ISO 9001) non è che si cambia da un giorno all'altro. Siamo abituati ad applicare le stesse procedure anche non essendo ancora certificati". [*]

[*] Frasi estrapolate dell'intervista ad Aldo Locurcio, responsabile del terminal intermodale di Segrate

L'impatto delle certificazioni è da ricercare sia nell'implementazione corretta delle procedure, sia nel rendere le procedure stesse più affidabili e corrette. Per quanto riguarda entrambe le dimensioni: attacchi e fornitura.

Partnership

Le relazioni che il terminal di Segrate ha con gli MTO sono di differenti tipologie.

Nello specifico con i clienti principali è attiva una partnership di lungo periodo, che nel tempo si è tradotta nella piena integrazione dei sistemi informativi delle aziende.

"Con CEMAT e IFB che sono i nostri maggiori clienti, abbiamo la piena compatibilità dei sistemi informativi. Quando per esempio facciamo un'accettazione e la aggiungiamo al nostro sistema automaticamente e istantaneamente l'informazione è disponibile anche per loro. La stessa cosa succede quando arriva un treno e possiamo fare la spunta ai contenitori per poi scaricarlo.

Inoltre loro girano automaticamente il nostro messaggio ai loro partner, così che per esempio chi deve venire a ritirare un contenitore che abbiamo scaricato è avvisato in tempo reale della disponibilità del contenitore pronto per il ritiro". [*]

Con le altre società il terminal di Segrate non ha questa forte integrazione e le informazioni vengono scambiate con meno tempestività.

L'impatto delle partnership è quindi rivolto alla sicurezza di fornitura e sicuramente implica una maggiore collaborazione e integrazione, ed evita anche possibili errori nell'invio e ricezione degli ordini essendo la procedura automatizzata.

Sviluppo della consapevolezza sulla sicurezza con i partner

Il terminal, dato l'ambito ristretto delle sue responsabilità, non si pome come riferimento per lo sviluppo della sicurezza nella filiera ed ha un rapporto con i propri clienti e fornitori strettamente operativo.

Riduzione della differenza di cultura tra azienda e partner

Come detto precedentemente, il terminal ha un rapporto con i propri clienti e fornitori strettamente operativo.

Focus sul cliente finale

Il terminal intermodale ha focus esclusivamente sul proprio fornitore e sul proprio cliente, e non lavora in ottica di filiera.

[*] Frasi estrapolate dell'intervista ad Aldo Locurcio, responsabile del terminal intermodale di Segrate

"Oltre alla responsabilità sul trasbordo, Il fatto che la merce arrivi più o meno in tempo al cliente finale e più o meno integra è un'informazione che noi non abbiamo e che non rientra nelle nostre responsabilità". [*]

Grado di importanza degli strumenti

Tra gli strumenti analizzati quello ritenuto indispensabile per ottenere performance sicure è stato individuato nella segnalazione di incidenti e debolezze.

Peso dei fattori causa

Per quanto riguarda la sicurezza da attacchi, che si traduce unicamente nei tentativi di furti nel terminal, la principale causa potenziale è l'errata/mancata implementazione delle procedure, in seconda battuta è la collusione; mentre l'inadeguatezza delle procedure è vista come ultima causa.

Per quanto riguarda la sicurezza di fornitura l'inadeguatezza del partner è stata individuata come la prima causa dei ritardi provocati nella filiera.

"Nel nostro lavoro il 90% delle volte che si verifica un ritardo è causato dallo spiombamento dei contenitori che riceviamo dall'operatore ferroviario, e dalle procedure che siamo obbligati a svolgere in queste situazioni". [*]

Come secondo fattore causa è stata individuata l'errata o mancata implementazione delle procedure operative, anche se è un aspetto molto più marginale.

"*Potrebbe capitare che si ha un danneggiamento dei container, e quindi un ritardo nella consegna, per problemi di movimentazione, cioè il gruista sbaglia una manovra con la gru, ad esempio andando in retro, e va contro un container".* [*]

Di seguito è riportata la tabella compilata durante l'intervista.

[*] Frasi estrapolate dell'intervista ad Aldo Locurcio, responsabile del terminal intermodale di Segrate

		SICUREZZA DA ATTACCHI			SICUREZZA DI FORNITURA			
		2	3	1	1	4	3	1
	Lo strumento viene utilizzato in azienda?	Collusione	Errata/mancata implementazione delle procedure	Inadeguatezza delle procedure	Mancata collaborazione / visibilità con i partner	Inadeguatezza partner	Errata/mancata implementazione delle politiche gestionali	Inadeguatezza delle politiche gestionali
Forza lavoro multidisciplinare	**NO**	↑						
Collaborazione tra dipendenti	**n.f.**		↓				↓	
Integrità, lealtà dei dipendenti	**NO**							
Sviluppo della consapevolezza interna sulla sicurezza	**n.f.**		↓				↓	
Aspetti soft	**f.**							
Continuous improvement	**NO**							
Business continuity planning	**NO**							
Segnalare incidenti e debolezze	**n.f.**						↓	
Knowledge management	**NO**							
Valutazione della conformità di sicurezza	**n.f.**		↓	↓			↓	↓
Partnership	**f.**				↓		↓	
Sviluppo della consapevolezza sulla sicurezza con i miei partner	**NO**							
Riduzione della differenza di cultura tra aziende e partner	**NO**							
Focus sul cliente	**NO**							

Evidenziati in giallo gli strumenti ritenuti indispensabili per ottenere performance sicure e i principali fattori che causano una minore sicurezza da attacchi e fornitura, la scala utilizzata per i fattori causa è in ordine crescente di importanza.

La risposta "n.f." sull'utilizzo dello strumento in azienda significa che lo strumento viene utilizzato in azienda ma non in maniera standard o formale.

D.13 VOTG

Tipologia azienda: trasporti ferroviari e intermodali

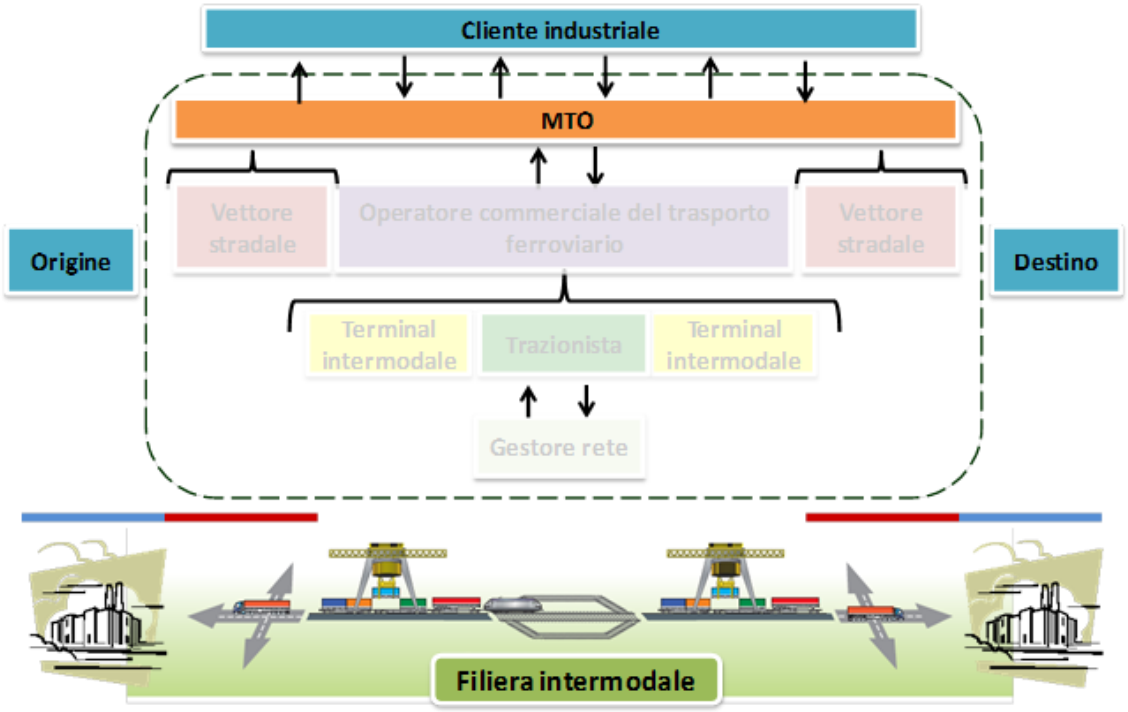
Area di responsabilità diretta: affitto tank container e gestione del rapporto cliente/fornitore

Fatturato: 144,5 mln €

Dipendenti: 107

Interlocutore: Giovanni Mazzali, Branch Office Manager di VOTG Tanktainer e rappresentante di VTG Italia S.r.l.

Sede intervista:VTG Italia S.r.l. c/o Uggiate Trevano (CO)



Premessa

VOTG Tankcontainer fa parte del gruppo tedesco VTG, che è leader mondiale per l'affitto di vagoni merci e di carri ferroviari. VTG possiede la più grande flotta privata di carri ferroviari in Europa e 50.000 vagoni merce in tutto il mondo. Oltre ai servizio di noleggio, VTG organizza il trasporto ferroviario e il trasporto intermodale di tank containers via strada, rotaia e nave. VTG è pertanto organizzata in 3 divisioni:

- Wagon Hire division: rappresenta il core business dell'azienda. VTG è fornitore di 1.000 tipologie diverse di vagoni merce, compatibili con il sistema ferroviario di tutti i Paesi. La flotta è costantemente in ampliamento, modernizzata e flessibile alle richieste dei clienti offrendo a loro un servizio affidabile e conforme alle regolamentazioni e al tipo di carico. VTG offre anche servizi di gestione e manutenzione di vagoni merce in Francia e Germania.
- Rail Logistics Division: VTG organizza il trasporto su rotaia in tutta Europa, servendosi della loro ampia rete internazionale di trazionisti. Il compito di VTG è quello di selezionare e coordinare di volta in volta il trazionista e i vagoni ferroviari.
- Tank Container Logistics: offre un servizio intermodale per il trasporto di tank containers, entro la quale si colloca VOTG Tankcontainer.

I clienti VTG sono le aziende del settore chimico, petrolifero, meccanico, agricolo e della carta.

Fondata nel 1951, VTG può vantare di una grande esperienza sull'intero processo del trasporto ferroviario e in particolare sul trasporto di prodotti liquidi e pericolosi.

VOTG tanktainer, nata nel 1997 da una joint venture tra VTG e Royal Vopak, fa parte del gruppo VTG. L'azienda offre un servizio intermodale per il trasporto di tank containers e ha a sua disposizione 6.500 tank container, di diverse tipologie. Questo tipo di ILU permette di essere trasportato con modalità door-to-door, su rotaia e su gomma senza che il contenuto venga toccato, garantendo un trasporto sicuro da origine a destinazione.

I tank container trasportano principalmente prodotti liquidi a temperatura controllata del settore chimico, petrolifero e dei gas compressi. VOTG è uno dei più grandi fornitori mondiali di servizi logistici per liquidi chimici, noto per la sua affidabilità e sicurezza. Tutte le procedure sono conformi agli standard S.Q.A.S. (Safety and Quality Assessment System) e alle certificazioni della Chemical Distribution Institute.

L'affidabilità del loro servizio è garantita invece dal sistema di tracking and tracing per ogni singolo container.

VOTG offre un servizio completo al cliente dalla pianificazione e alla supervisione del trasporto, non che del trasporto stesso. La supply chain del tank container viene progettata in base alle esigenze del singolo cliente. VOTG seleziona la tipologia di container più adatta al carico che vi deve essere trasportato e organizza il trasporto da origine a destinazione. Nel trasporto su rotaia si occupa anche della relazione con i partner trazionisti.

Oltre a organizzare il trasporto della propria flotta, VOTG gestisce anche le flotte esterne e offre soluzioni per i clienti che chiedono il ridisegno di una supply chain efficiente.

Il contributo di Giovanni Mazzali offre un punto di vista non strettamente operativo, occupandosi in VOTG dell'aspetto commerciale, ma al contrario offre una visione ad alto livello dell'intero processo.

Adozione degli strumenti

Essendo VOTG una società di servizi e non avendo del personale coinvolto operativamente nel processo di trasporto, alcuni strumenti non possono essere argomento dell'intervista.

Aspetti soft

"La cultura è la chiave di successo dell'azienda. Non basta applicare le procedure, bisogna avere una cultura aziendale".[*]

VTG group conta quasi 1.000 dipendenti in tutto il mondo, tutti accomunati dalla stessa cultura, espressa da un codice di condotta e da una chiara vision aziendale, messi in evidenza sul sito della società.

Al codice di condotta fanno riferimento tematiche quali conformità alle leggi, lealtà competitiva, lealtà e tutela del personale, protezione dei dati e delle informazioni, sicurezza e ambiente. I *Corporate values* fanno leva invece sulla qualità, la sicurezza e l'affidabilità del servizio.

Il modo di operare, dettato dal codice di condotta, è uguale per tutte le filiali del mondo. Se qualcosa non è chiaro, VTG invita i dipendenti a far riferimento ai propri superiori.

[*] Frasi estrapolate dell'intervista a Giovanni Mazzali, Branch Office Manager di VOTG

*"Difficilmente ci sono casi in cui un dipendente "illuminato" dal motto e dai valori aziendali evidenzino lacune nelle procedure; piuttosto accade grazie alla sua esperienza operativa".**

La diffusione di una cultura chiara e ben definita, ha riscontro soprattutto nell'operatività e nella lealtà e integrità dei dipendenti.

Continous improvement

VOTG incentiva i suoi dipendenti e collaboratori d assumere un atteggiamento propositivo e dare consigli o suggerimenti per rendere il processo più efficiente e sicuro.

*"Esiste un processo di miglioramento continuo che parte dall'investigazione dei punti deboli e procede con l'implementazione di nuove procedure. I nostri operatori sono incentivati a far notare i punti deboli non ai fini di un riconoscimento economico: ne giova l'azienda ma soprattutto chi ci lavora perché le modifiche delle procedure vengono accettate e assimilate meglio se provenienti dagli stessi che le mettono in atto".**

In VOTG esiste quindi sia un processo formale di controllo, sia un processo di miglioramento continuo che deve la sua realizzazione al flusso informativo che va dal basso verso l'alto, spinto non da ragioni economiche ma da un senso di appartenenza all'azienda e di collaborazione degli operatori.

In questo senso il miglioramento continuo si estende anche al di fuori dei confini aziendali e impatta sull'adeguatezza dei partner di VOTG.

Business continuity planning

In VOTG è presente un piano formale di gestione degli imprevisti più ricorrenti che viene costantemente aggiornato e reso disponibile a chi si occupa della pianificazione del trasporto.

*"Esistono procedure formali per ovviare a diverse problematiche. Al verificarsi di ogni nuova problematica, il piano viene aggiornato".**

Come evidenziato sul sito aziendale, VOTG offre supporto formale in caso di problematiche tramite una linea guida per le procedure standard da applicare in caso di emergenze, chiamata "*Guideline for the standard procedure of dealing with Emergency response issues*".

* Frasi estrapolate dell'intervista a Giovanni Mazzali, Branch Office Manager di VOTG

Segnalare incidenti e debolezze

Come già discusso, le segnalazioni delle debolezze presenti nel sistema e nelle procedure è alla base del piano di continuous improvement, ampiamente promosso dall'azienda.

"VOTG riceve e analizza le lamentele del cliente per andare a capire quali procedure o politiche aziendali possono essere migliorate. È la prima leva per il miglioramento".[*]

Per quanto riguarda la segnalazione degli incidenti, essa viene fortemente consigliata dal momento che in caso di mancata segnalazione VOTG mette in gioco il rapporto del collaboratore con l'azienda.

"L'autista prima di caricare il contenitore lo controlla sempre. Se qualcosa non va deve venire segnalato. Tutti i trazionisti sanno che devono chiamare sempre in caso di problemi, ed essendoci un rapporto familiare con i nostri partner, questo comportamento viene naturale. La mancata segnalazione di un incidente può portare fino al licenziamento".[*]

Nonostante VOTG tenda a instaurare un rapporto famigliare con suoi partner, la procedura di segnalazione degli incidenti e debolezze è piuttosto formale. Anche grazie ai sistemi di tracking and tracing, esiste un forte controllo degli operatori e dei propri container.

"L'operatore si sente controllato perché sa che verranno segnalati tutti gli incidenti e si può risalire a lui in caso di comportamento collusivo". [*]

Con un processo formale e costante di segnalazione è possibile effettuare un'attenta analisi degli incidenti e dei near messes dalla quale è possibile risalire alla mancata o errata implementazione delle procedure.

A testimonianza della formalità del processo e della sua importanza, sul sito aziendale, tra le aree entro le quali l'azienda esercita un rigido controllo, in primis viene proprio indicata quella di "*Safety Incidents*" e a seguire i casi di "*non-performance*".

Knowledge management

In VOTG non viene utilizzato un vero e proprio software per la gestione della conoscenza; tuttavia viene fatto uno sforzo di formalizzazione delle conoscenze e delle esperienze cumulate, che vengono messe per iscritto e rese disponibili a chi pianifica.

"La formalizzazione della conoscenza viene adottata in particolar modo a livello manageriale e può essere utile per il miglioramento delle procedure. Impatta sulla

[*] Frasi estrapolate dell'intervista a Giovanni Mazzali, Branch Office Manager di VOTG

visibilità del mio partner, non intesa come stato di avanzamento, bensì come conoscenza delle pratiche che il mio partner utilizza in certe situazioni". *

Valutazione della conformità di sicurezza

VOTG garantisce un servizio conforme alle leggi e regolamentazioni di ogni Paese e ai requisiti ambientali e di sicurezza. Nello specifico tutte le procedure sono conformi agli standard S.Q.A.S (Safety Quality Assessment System) e certificate dalla Chemical Distribution Institute.

Inoltre si serve di collaboratori a loro volta certificati, messo in luce sul sito aziendale parlando di "*Assessment of subcontractors according to the rules set out by our quality handbook*".

"Anche le stazioni di lavaggio dei tank container, che offrono un servizio fondamentale in questo campo, devono eseguire la pulitura delle cisterne secondo gli standard definiti per legge in base alla tipologia di liquido trasportato". *

Partnership

La collaborazione con i partner è di forte intensità per quanto riguarda i padroncini e di modesto livello con i trazionisti, nonostante questi ultimi siano delle figure solitamente indipendenti nella filiera dell'intermodale.

I padroncini lavorano esclusivamente per VOTG per cui devono rispettare i criteri imposti dall'azienda e attenersi al codice comportamentale. Da questo rapporto esclusivo VOTG ottiene sicuramente parecchi vantaggi, ma nonostante la mancanza di mezzi propri esiste sempre il rischio di non avere mezzi per rispondere alle emergenze, seppur esista una stretta collaborazione e forte visibilità sull'azienda di trasporto.

Per quanto riguarda il rapporto con i trazionisti, VOTG, facendo parte del gruppo VTG che è fornitore di vagoni ferroviari e organizzatore del trasporto ferroviario, riesce ad essere più di altre aziende del settore strettamente legato a questo attore della filiera.

VOTG attraverso relazioni di lungo periodo, una forte collaborazione, un sistema di condivisione di rischi e premi e lo sviluppo della fiducia con i partner, riesce in primo luogo a disincentivare qualsiasi comportamento collusivo nei suoi confronti.

"La forza dell'azienda, oltre che nella cultura, sta anche nelle relazioni con i propri partner che sono di lungo periodo e solide. In più si è sviluppata una gestione chiara e di tipo "familiare" che evita comportamenti opportunistici". *

* Frasi estrapolate dell'intervista a Giovanni Mazzali, Branch Office Manager di VOTG

La stretta relazione con i partner fa si che gli strumenti di continuous improvement e knowledge management vengano condivisi anche da loro, i quali collaborano per un miglioramento delle procedure attraverso le loro competenze.

Sviluppo della consapevolezza sulla sicurezza con i partner

Oltre alle certificazioni, VOTG impone ai partner un preciso metodo di lavoro che garantisca qualità, affidabilità e sicurezza, in accordo ai propri *Corporate Values*.

"Lo sviluppo della consapevolezza, intesa come garanzia di sicurezza per il trasporto, è un aspetto prioritario e chiave per VOTG. Esiste una funzione interna preposta per la formazione dei partner sulle tematiche di sicurezza. VOTG fa anche controlli periodici sull'adeguatezza del partner e dell'equipaggiamento a loro disposizione".[*]

VOTG non si impegna quindi in prima persona nella formazione e training degli operatori, compito che è assegnato alle aziende partner. Tuttavia detta le linee guida e si pone come punto di riferimento della filiera per l'adozione di pratiche di sicurezza e divulgatore di una cultura di sicurezza, come lo dimostra il motto *"*If you can't manage it safely, don't manage it at all!".

Riduzione della differenza di cultura tra azienda e partner

VOTG lavorando su scala mondiale, considera l'importanza non solo di una riduzione delle differenze culturali tra partner e azienda, ma anche tra le filiali stesse.

"Il rapporto ormai familiare con i nostri partner ci aiuta a ridurre le differenze, quindi ci permette di lavorare meglio, far circolare di più le informazioni e di aumentare la trasparenza". [*]

Una solida partnership comporta sempre azioni volte alla riduzione delle differenze, con lo scopo non solo di assicurarsi un partner affidabile e adeguato dal punto di vista delle competenze tecniche, ma soprattutto dal punto di vista relazionale. Azioni specifiche vengono implementate da VOTG una tantum, senza una modalità strutturata.

Focus sul cliente finale

La collaborazione di VOTG è forte con i partner, ma ancor di più con i suoi clienti anche se non esistono incentivi riconosciuti dal cliente finale alla filiera intermodale.

VOTG svolge un ruolo di alto livello nella gestione di tutto il rapporto tra fornitore-cliente. Il suo compito è proprio quello di disegnare l'intera supply chain in relazione alle esigenze del cliente. Per ogni singola relazione sceglie i partner affinché siano in

[*] Frasi estrapolate dell'intervista a Giovanni Mazzali, Branch Office Manager di VOTG

grado in primis di offrire un servizio adeguato e conforme alle richieste del cliente e li orienta verso un obiettivo comune, ossia la soddisfazione del cliente finale. VOTG si impegna nel condividere un obiettivo comune orientato al cliente tra i suoi partner.

Grado di importanza degli strumenti

Da quel che risulta dalla nostra intervista, la diffusione della cultura di sicurezza e il miglioramento continuo sono sicuramente un *must* aziendale.
Nel sito aziendale vengono elencate sei aree entro le quali l'azienda si impegna a tenere un rigido controllo per il mantenimento di un focus sul quality management:

- Safety Incidents
- Non-performances
- Assessment of subcontractors according to the rules set out by our quality handbook
- Subcontractor and depot guidelines
- Guideline for the handling of equipment / product claims
- Guideline for the standard procedure of dealing with Emergency response issues

Attraverso queste sei aree, ma anche la nostra intervista, deduciamo anche l'importanza che ricoprono gli strumenti di valutazione della conformità di sicurezza, di segnalazione di incidenti e debolezze e di sviluppo della consapevolezza di sicurezza con i partner.

Peso dei fattori causa

Per quanto riguarda la sicurezza da attacchi i fattori causa identificati in ordine di importanza di impatto sulla prestazione finale sono l'inadeguatezza procedure, l'errata e mancata implementazione delle stesse e infine la collusione.
Per quanto riguarda la sicurezza di fornitura invece, in ordine di importanza sono state individuate l'inadeguatezza politiche gestionali, l'inadeguatezza del partner, la mancata visibilità sul partner e infine l'errata implementazione delle procedure.

Di seguito è riportata la tabella compilata durante l'intervista.

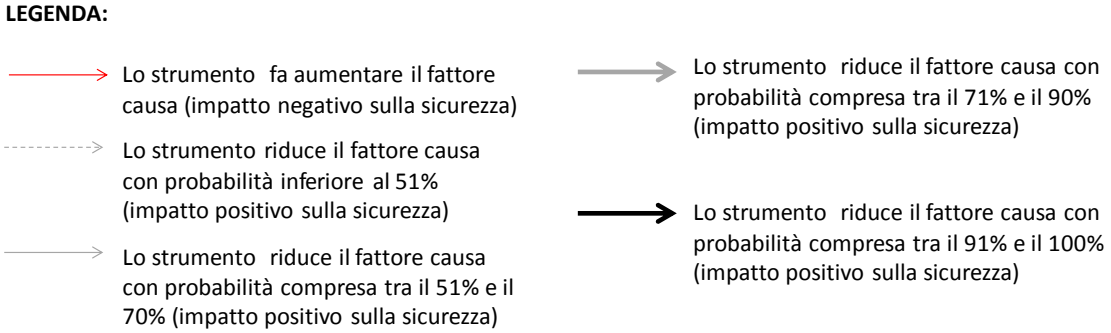
		SICUREZZA DA ATTACCHI			SICUREZZA DI FORNITURA			
		1	2	3	2	3	1	4
	Lo strumento viene utilizzato in azienda?	Collusione	Errata/mancata implementazione delle procedure	Inadeguatezza delle procedure	Mancata collaborazione / visibilità con i partner	Inadeguatezza partner	Errata/mancata implementazione delle politiche gestionali	Inadeguatezza delle politiche gestionali
Forza lavoro multidisciplinare								
Collaborazione tra dipendenti								
Integrità, lealtà dei dipendenti								
Sviluppo della consapevolezza interna sulla sicurezza								
Aspetti soft	**f.**	↓	↓				↓	
Continuous improvement	**f.**			↓		↓		↓
Business continuity planning	**f.**					↓		↓
Segnalare incidenti e debolezze	**f.**	↓	↓	↓		↓	↓	↓
Knowledge management	**n.f.**			↓	↓	↓		↓
Valutazione della conformità di sicurezza	**n.f.**			↓		↓		↓
Partnership	**f.**	↓		↓	↓	↓		↓
Sviluppo della consapevolezza sulla sicurezza con i miei partner	**f.**	↓		↓		↓		↓
Riduzione della differenza di cultura tra aziende e partner	**n.f.**	↓			↓	↓		
Focus sul cliente	**n.f.**				↓		↓	↓

Evidenziati in giallo gli strumenti ritenuti indispensabili per ottenere performance sicure e i principali fattori che causano una minore sicurezza da attacchi e fornitura, la scala utilizzata per i fattori causa è in ordine crescente di importanza.

La risposta "n.f." sull'utilizzo dello strumento in azienda significa che lo strumento viene utilizzato in azienda ma non in maniera standard o formale

E. Mappe causali in funzione dei fattori di contesto

Legenda:

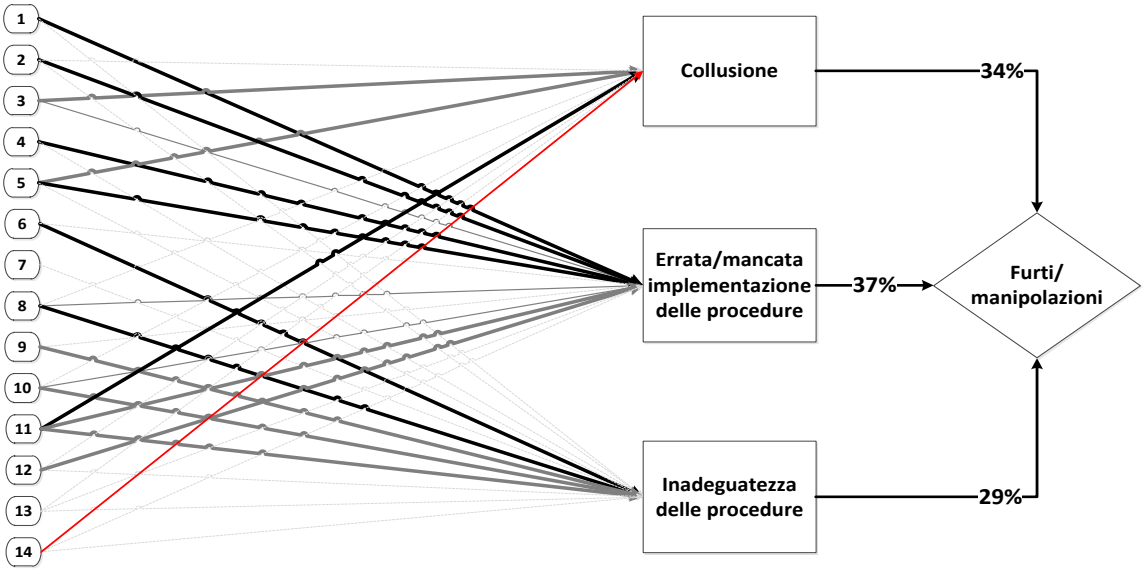


(1) Forza lavoro multidisciplinare
(2) Collaborazione tra dipendenti
(3) Integrità, lealtà dei dipendenti
(4) Sviluppo della consapevolezza interna sulla sicurezza
(5) Aspetti soft
(6) Continuous improvement
(7) Business continuity planning
(8) Segnalare incidenti e debolezze
(9) Knowledge management
(10) Valutazione della conformità di sicurezza
(11) Partnership
(12) Sviluppo della consapevolezza sulla sicurezza con i miei partner
(13) Riduzione della differenza di cultura tra aziende e partner
(14) Focus sul cliente

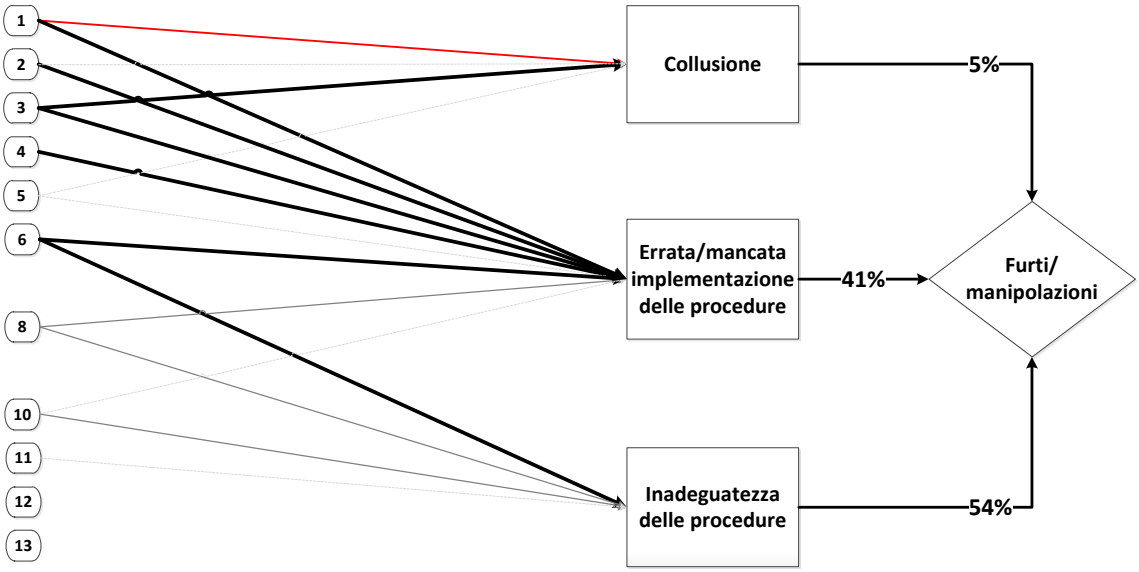
E.1 Dimensione

Attacchi

Grande



Piccola



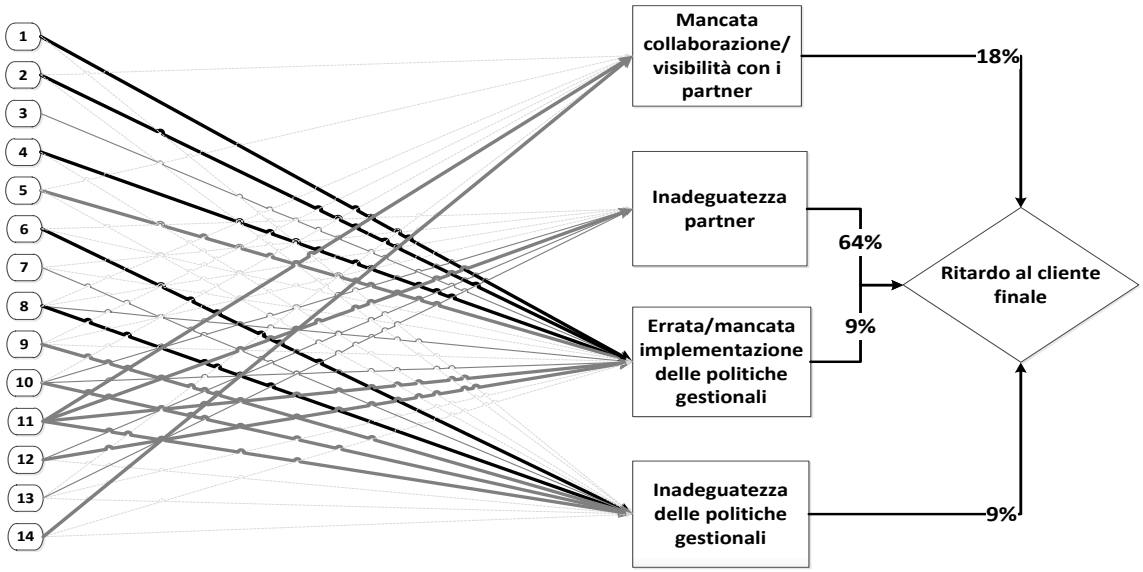
In figura si evidenzia il fatto che le grandi aziende segnalano il trade-off tra lo strumento 14-focus sul cliente finale e il KPI furti/manomissioni (attraverso un aumento della collusione), mentre le aziende di dimensione minore segnalano il trade-off che coinvolge lo stesso KPI ma in relazione allo strumento 1-forza lavoro multidisciplinare. Questa differenza risiede nel diverso orientamento delle due tipologie di aziende: mentre le piccole aziende fanno considerazioni a livello più operativo (un

cl

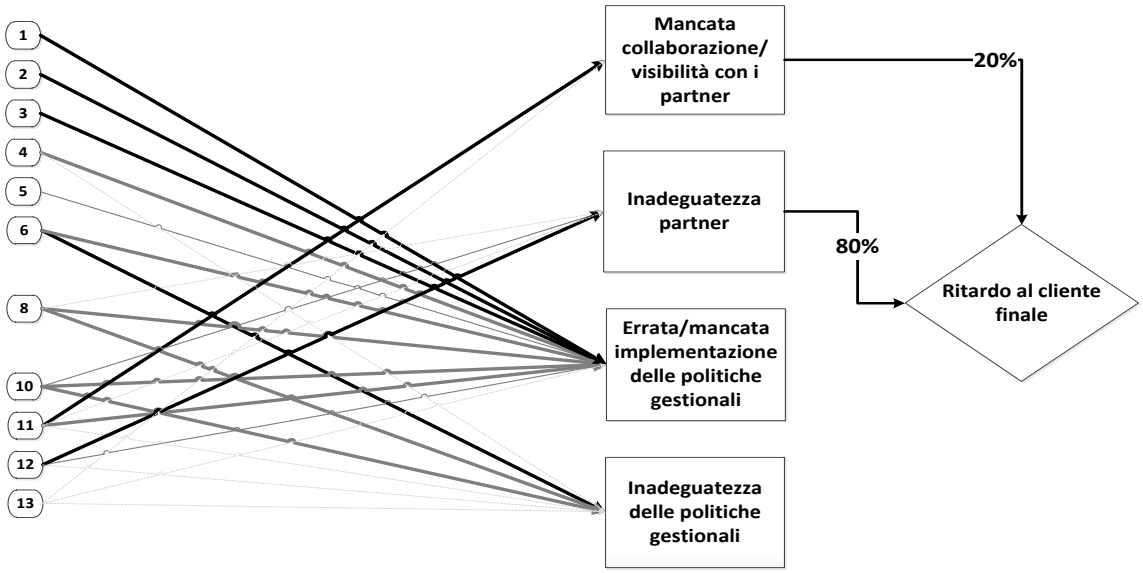
operatore che ha conoscenze ad ampio spettro potrebbe individuare i punti deboli del processo e, agendo in malafede, attuare un piano collusivo), le grandi aziende si soffermano di più su considerazioni di filiera (se i partner conoscono meglio il processo nella sua totalità potrebbero individuare eventuali punti deboli della filiera e attuare un piano collusivo). Una forte differenza tra queste due tipologie di aziende è anche il differente impatto del fattore causa collusione sul KPI di sicurezza: l'impatto è molto maggiore per le aziende di grandi dimensioni. Il motivo è da ricercare nel rapporto più stretto a livello personale, che può instaurarsi in una piccola azienda, tra operatori e management per consentire un controllo diretto sui dipendenti (cosa che diventa molto difficile con l'aumento delle dimensioni).

Fornitura

Grande



Piccola



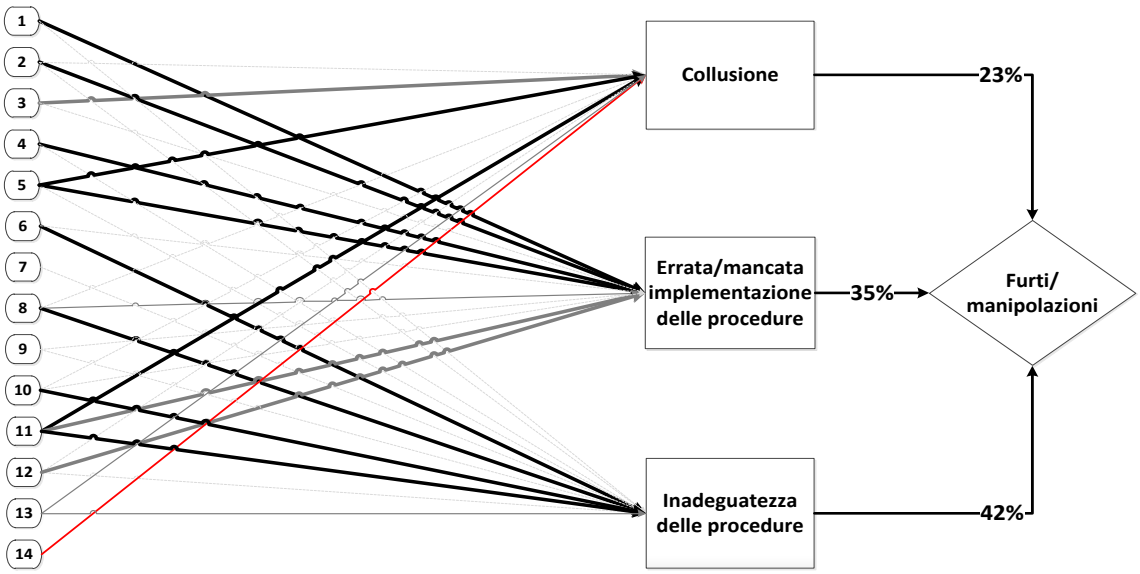
Si nota come impattino molto di più i fattori causa esterni di mancata collaborazione/visibilità e inadeguatezza dei partner e si evidenza come questo derivi dal fatto che gli strumenti proposti abbiano meno impatti proprio su questi fattori causa. Questa considerazione è valida per le grandi aziende e si segnala come si accentui al diminuire della dimensione. Il motivo risiede nel fatto che le grandi aziende hanno un numero maggiore di leve per influenzare i partner (maggior potere contrattuale) e hanno quindi la possibilità di attutire questo fenomeno.

Si nota, sia per quanto riguarda la sicurezza di attacchi che per quella di fornitura, come le aziende di grandi dimensioni applichino un maggior numero di strumenti culturali da noi proposti e abbiano conseguentemente degli impatti maggiori.

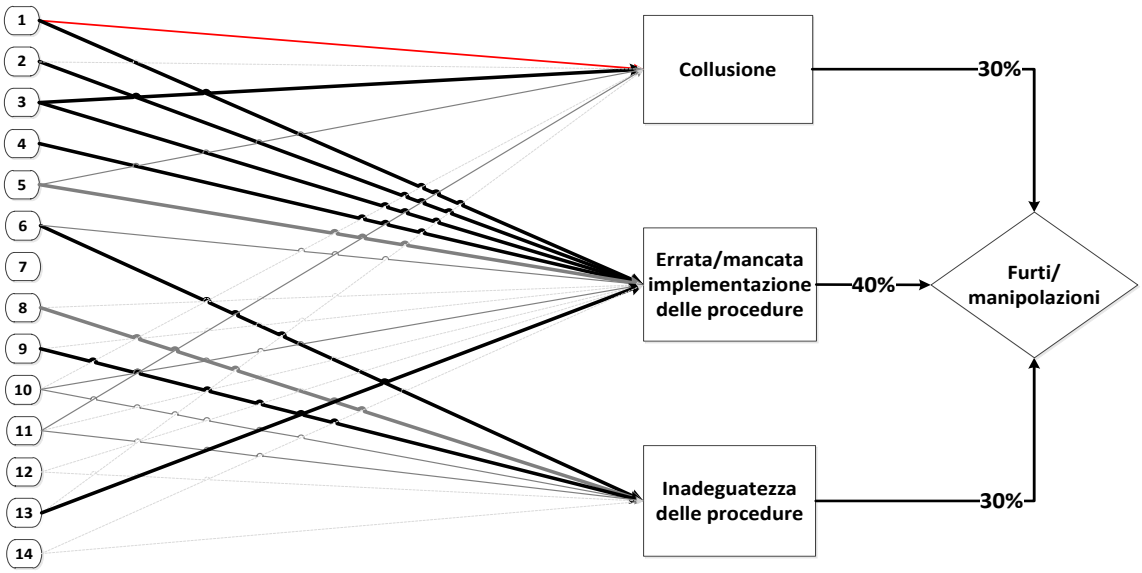
E.2 Integrazione

Attacchi

Alta



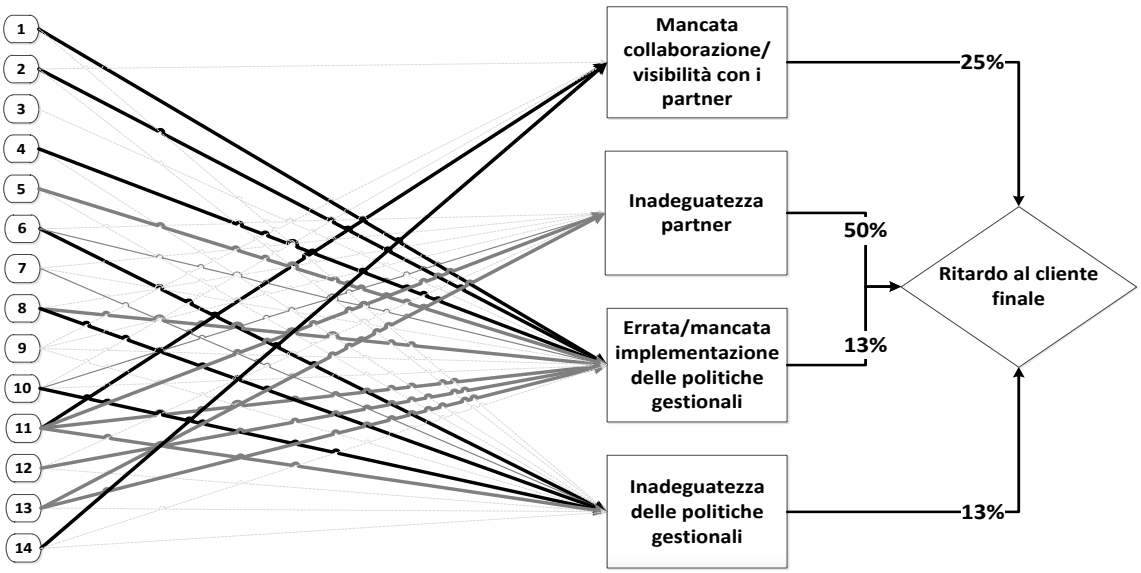
Bassa



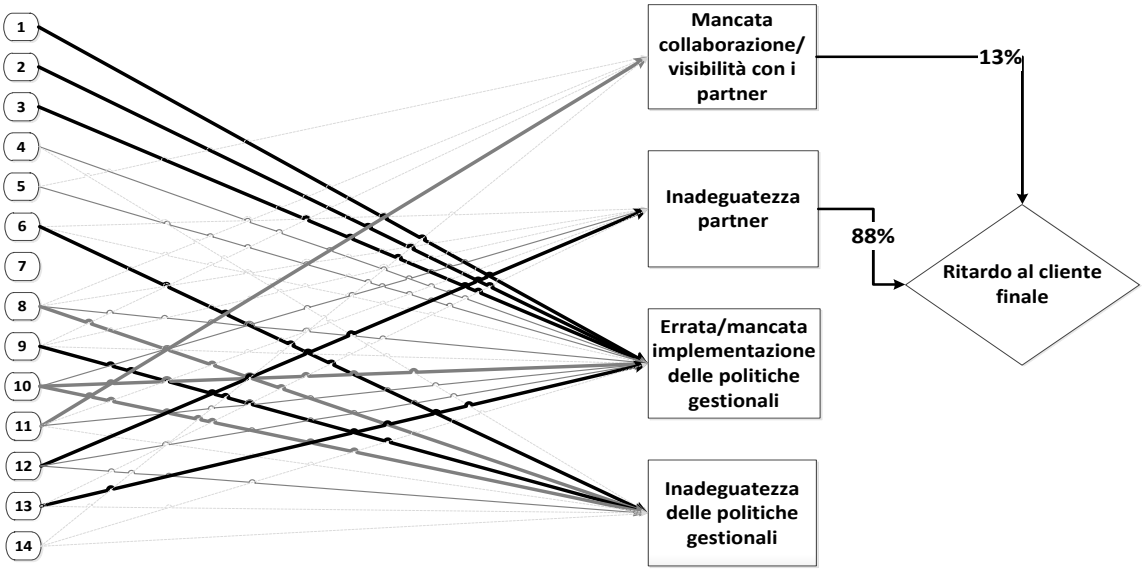
Per quanto riguarda la sicurezza da attacchi non si presentano nette distinzioni tra le due mappe causali, sia per quanto riguarda l'utilizzo e l'impatto degli strumenti, sia per quanto riguarda il peso dei fattori causa sul KPI.

Fornitura

Alta



Bassa



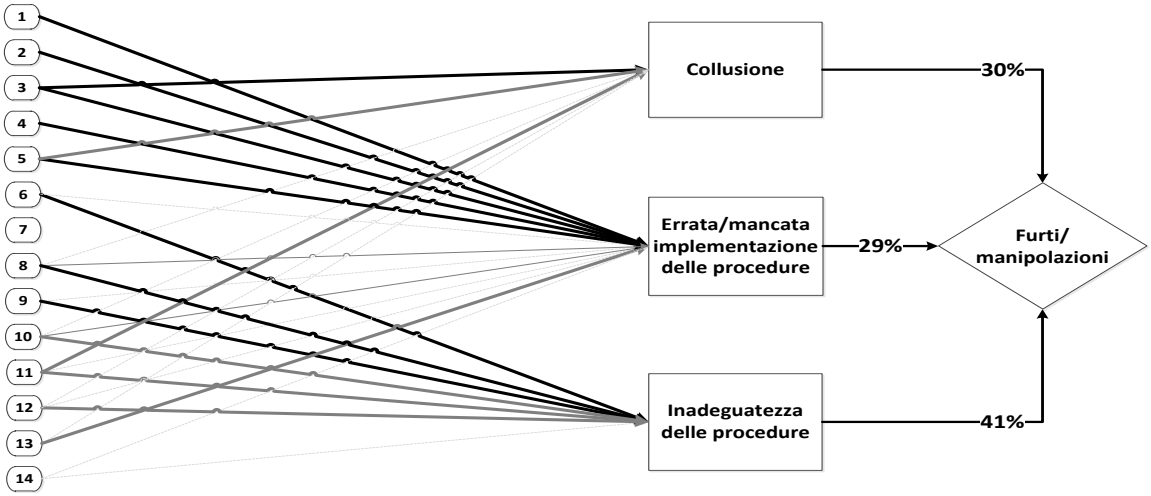
Anche per la sicurezza di fornitura non esistono sostanziali differenze in funzione della diversa integrazione verticale. L'unica differenza si può notare nel peso dei fattori causa i quali sono maggiormente sbilanciati per le aziende poco integrate: per queste aziende i

fattori causa esterni sono i soli che spiegano la prestazione del KPI “ritardo al cliente finale”.

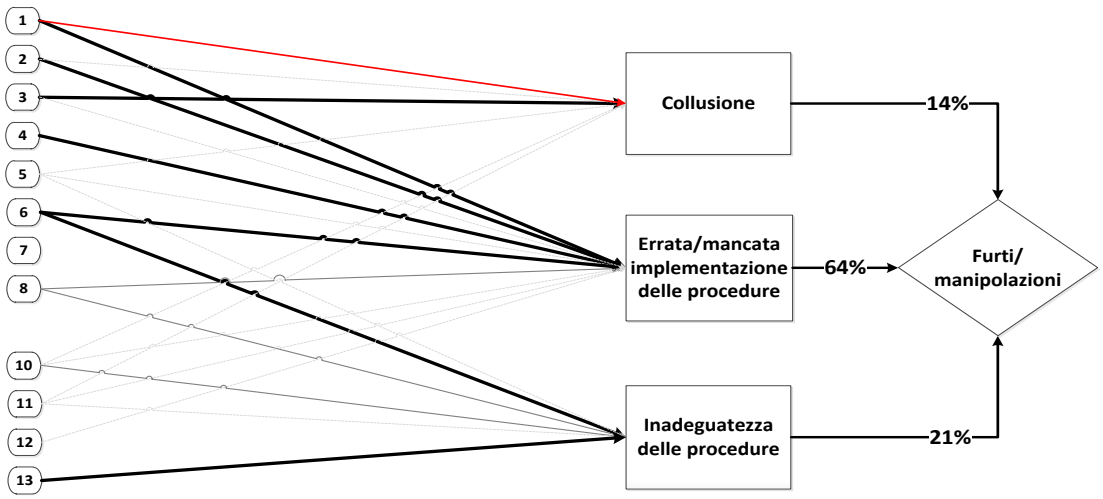
E.3 Ambito

Attacchi

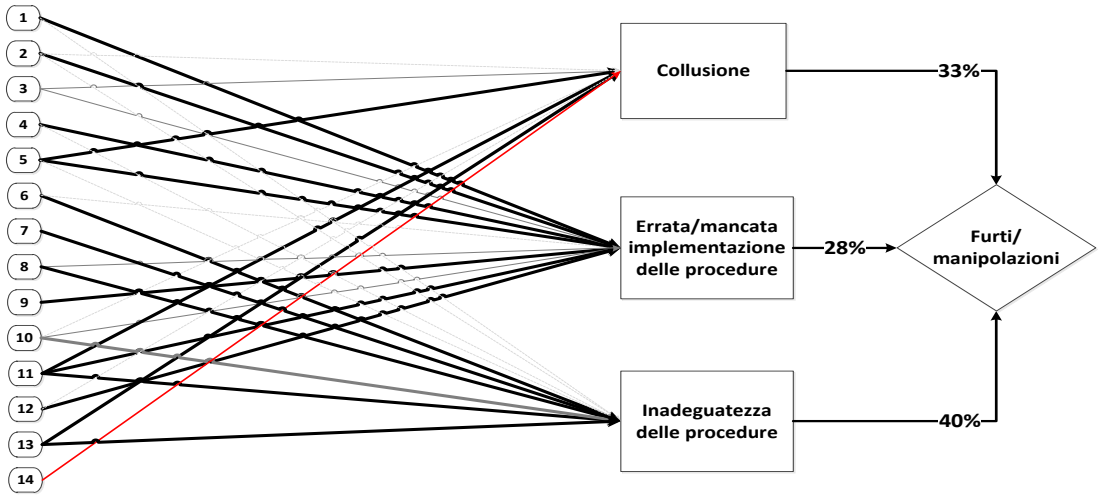
Strada



Ferrovia



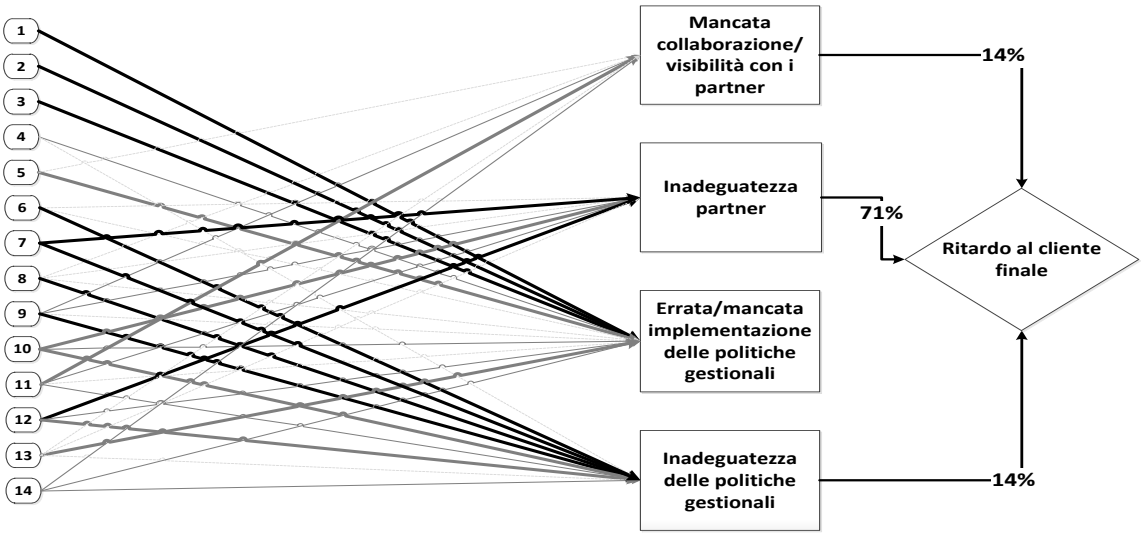
Strada-Ferrovia



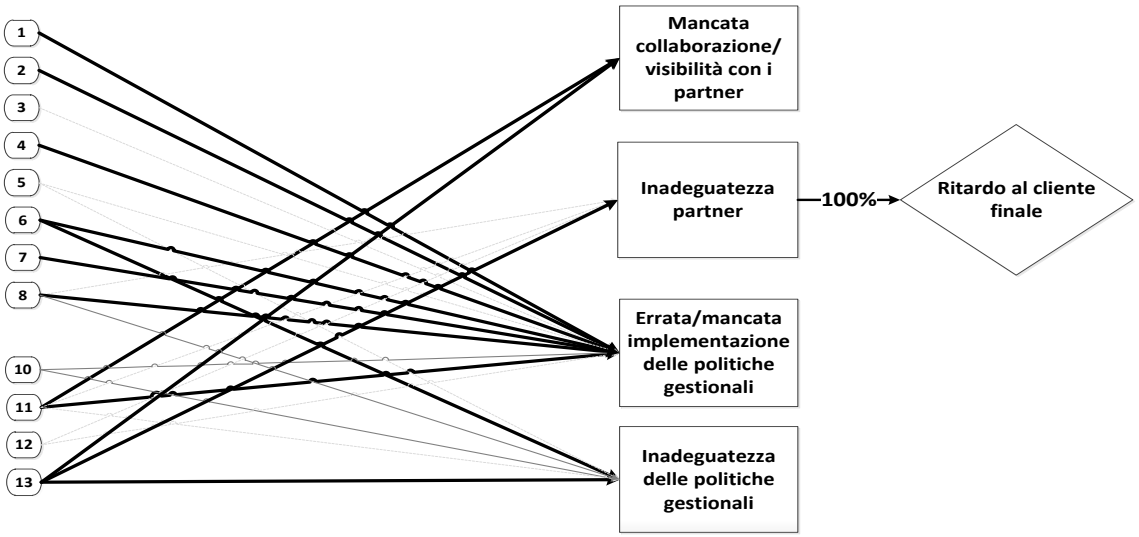
Si nota come vi sia una differenza sostanziale per strumenti di tipo esterno (10,11,12,13,14), dal momento che gli impatti sul KPI "furti/manipolazioni" di questi risultano maggiori per aziende con interfaccia stradale. Si evidenzia inoltre il fatto che le aziende con interfaccia ferroviaria rilevano come più importante il fattore causa "errata/mancata implementazione delle procedure"; il motivo è da attribuire alla numerosità ed eterogeneità delle attività che gli operatori di queste aziende devono svolgere contestualmente (si pensi ai numerosi controlli da effettuare all'arrivo e durante il trasbordo della merce in un terminal).

Fornitura

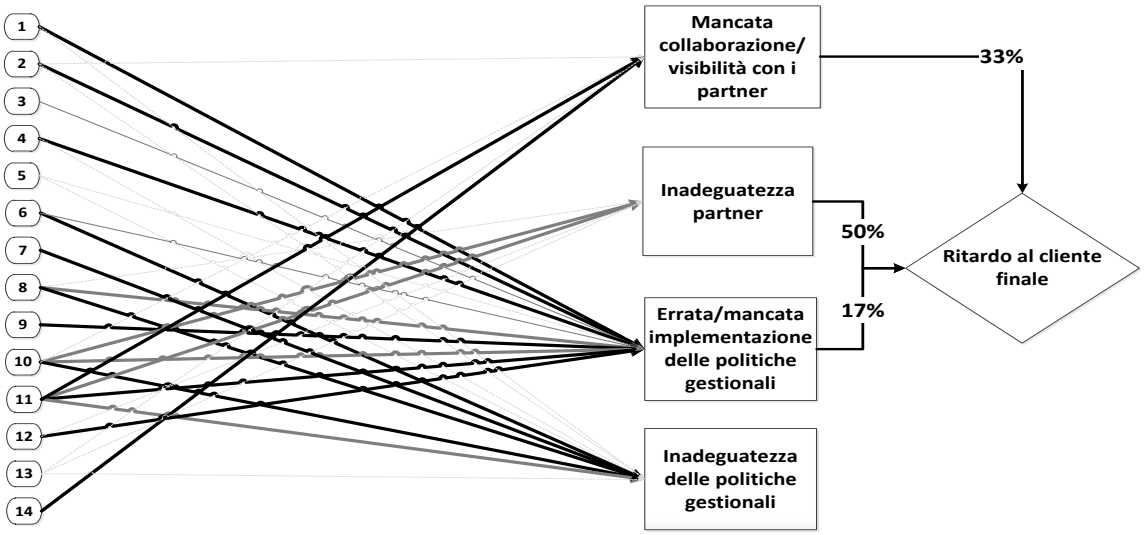
Strada



Ferrovia



Strada-Ferrovia



Per quanto riguarda il KPI "ritardo al cliente finale" si sottolinea il fatto che tutte le aziende con interfaccia ferroviaria abbiano indicato come unica causa l'inadeguatezza del partner; per l'interfaccia stradale (anche se questa rimane la causa principale) si sommano "mancanza di collaborazione/visibilità con i partner" e "inadeguatezza delle politiche gestionali". Siccome le cause più comuni di ritardo sono da attribuire al trazionista ferroviario, la motivazione risulta essere che le imprese con interfaccia ferroviaria sono le più esposte a questa eventualità; per le imprese stradali, invece, subentrano cause come la mancanza di collaborazione/visibilità che limitano la tempestività delle informazioni per consentire l'attuazione di piani alternativi.

Bibliografia

Asree S., Zain M., Razalli M.R. (2010) – "Influence of leadership competency and organizational culture on responsiveness and performance of firms", International Journal of Contemporary Hospitality Management (Vol. 22 No. 4, pp. 500-516)

Autry C.W., Bobbitt L.M. (2008) – "Supply chain security orientation: conceptual development and a proposed framework", The International Journal of Logistics Management (Vol. 19 No. 1, pp. 42-64)

Bajpai K. (2003) - "The idea of human security", International Studies (Vol. 40 No. 3, pp. 195-228)

Barrow J.C. (1977) - "The variables of leadership: a review and conceptual framework", Academy Management Review (April, pp. 231-51)

Benson A.S. (2005) – "The role of organizational culture in creating secure and resilient supply chains", Degrees of Master of Science in Transportation and Master of Engineering in Logistics, MIT

Black S.A., Porter L.J. (1996) - "Identification of the critical factors of TQM", Decision Sciences (Vol. 27 No. 1, pp. 1-21)

Bonazzi G. (2002) - "Storia del pensiero organizzativo", Franco Angeli Editore

Bowersox D.J., Closs D.J., Stank T.P. (2003) - "Understanding and mastering cross-enterprise collaborative supply chain management", Supply Chain Management Review (Vol. 7 No. 4, pp. 18-29)

Burmeisters A., Solovjovs D. (2009) - "Security Solutions of Supply Chain Management", Acta Techinca Jaurinensis Series Logistica (Vol. 2 No. 3, pp. 361-366)

Catino M. (2002) - "Da Chernobyl a Linate", Edizione Carocci

Closs D.J., McGarrel E.F. (2004) – "Enhancing security throughout the supply chain", Special report series of IBM Center for the business of Government

Closs D.J., Speier C., Whipple J. and Voss M.D. (2008) - "A framework for protecting your supply chain", Supply Chain Management Review (Vol. 12 No. 2, pp. 38-45)

Commissione dell'Unione Europea (28 marzo 2011) – "Libro Bianco: tabella di Marcia verso uno spazio europeo dei trasporti per una politica dei trasporti competitive e sostenibile", Bruxelles

Commissione dell'Unione Europea (24 novembre 2006) - "Regolamento (CE) n. 1692/2006 del Parlamento europeo e del Consiglio" (Gazzetta Ufficiale dell'Unione europea serie L 328), Bruxelles

Commissione dell'Unione Europea, Conferenza Europea dei Ministri dei Trasporti, Commissione Economica per l'Europa delle Nazioni Unite (2001) – "Terminology on combined transport", New York , Genova

Confederazione generale italiana dei trasporti e della logistica (febbraio 2000) - "L'operatore in trasporto multimodale (MTO) e l'operatore logistico (LO)" (quaderno n. 88/2)

Crist P., Crass M., Miyake M. (2005) – "Container transport security across modes"– OECD e EMCT final report

Daschkovska K. (2010) – "Description of ILU's supply chain processes", IMCOSEC, deliverable 1.1

Daschkovska K., Scholz-Reiter B. (2008) – "Electronic Seals for Efficient Container Logistics", BIBA University Brema, IGSDL University Brema

Debernardi A. (1997) - "Integrazione modale e integrazione nodale: questioni organizzative", KINEO (No.13, pp. 8-9)

Dean J.W.J., Bowen D.E (1994) - "Management theory and total quality: improving research and practice through theory development", Academy of Management Review (Vol. 19, pp. 392-418)
Desphande R., Webster F.E. (1989) - "Organizational culture and marketing: defining the research agenda", Journal of Marketing (Vol. 6 No. 2, pp. 204-223)

Downey L. (2006) – "International Cargo Conudrum", RFID Journal

Donner M., Kruk C. (2009) - "Supply chain security guide", Department for International Development

Eggers W.D. (2004) - "Prospering in the secure economy", Deloitte Research Study

Fairchild H.P. (1944) – "Dictionary of Sociology", Philosophy Library, New York, NY.

Fisher R.J., Green G. (2004) – "Introduction to Security", 7th ed., Elsevier

Freight Leader Council (novembre 2009), "Il trasporto intermodale combinato in italia possibili interventi di sostegno" (Quaderni numero 19)

Garrido S., Machado V.H. (2009) – "Strategies to mitigate supply chain disturbances", NECE, Department of Management and Economics University of Beira Interior, Covilhã, Portugal

Gould J. (2007/2008) - "Supply chain security: an overview of theoretical applications", Research report 2007/2008 of IGSDL (pp. 26-28)

Gerencser M., Weinberg J., Vincent D. (2002) - "Port Security War Games: Implications For US Supply Chain", Booz Allen Hamilton

Goetz J. P., LeCompte M. D. (1984) – "Ethnography and qualitative design in educational research", New York: Academic Press

Gunasekaran A., McGaughey R.E. (2003) - "TQM in supply chain management", The TQM Magazine (Vol. 15 No. 6, pp. 361-3)

Gutierrez X., Hintsa J. (2006) – "Voluntary supply chain security programs: a systematic comparison", Cross-border Research Association, Losanna

Harrald J., Stephens H.W., van Dorp J.R. (2004) – "A framework for sustainable port security", Journal of Homeland Security and Emergency Management (v1,issue 2, article 12)

Heinrich H.W (1932) – "Industrial Accident Prevention: A Scientific Approach", McGraw-Hill, New York.

Hess K.M., Wrobleski H.M. (1996) – "Introduction to Private Security", 4th ed., West Publishing Company, Saint Paul, MN.

IMCOSEC, European Commission (2010) – "Description of Work", Annex I,

Jia F., Rutherford C. (2010) – "Mitigation of supply chain relational risk caused by cultural differences between China and the West", The International Journal of Logistics Management (Vol. 21 No. 2, pp. 251-270)

Jüttner U. (2005) - "Supply chain risk management: understanding the business requirements from a practitioner perspective", International Journal of Logistics Management (Vol. 16 No. 1, pp. 120-141)

Jüttner U., Peck H., Christopher M. (2003) - "Supply chain risk management: outlining an agenda for future research", International Journal of Logistics: Research and Applications (Vol. 6 No. 4, pp. 197-210)

Kim S.J., Deng G., Gupta K.S. (2009) - "Enhancing cargo container security during transportation: a mesh networking based approach", Arizona State University, Tempe (Arizona)

Knight P. (2003) – "Supply chain security guidelines", IBM Corporation

Lacey D. (2009) – "Managing the Human Factor in Information Security", Wiley Editore, Londra.

Lacey D. (2010) – "Understanding and trasforming organizational security culture", Information Management & Computer Security (Vol. 18 No. 1, pp. 4-13)

Lau C.M., Ngo H.Y. (1996) - "One country many cultures: organizational cultures of firms of different country origins", International Business Review (Vol. 5 No. 5, pp. 469-86)

Lee H.L., Wolfe M.L. (2003) - "Supply chain security without tears", Supply Chain Management Review (Vol. 7 No. 1, pp. 12-20)

Lin X.H., Germain R. (1999) - "Predicting international joint venture interaction frequency in US-Chinese ventures", Journal of International Marketing (Vol. 7 No. 2, p. 5)
Lin X.H. (2004) - "Determinations of cultural adaptation in Chinese-US joint ventures", Cross Cultural Management, (Vol. 11 No. 1, p. 35)

Maslow A.H. – "Motivazione e personalità", (1954)

Mazzarino M., (1998) - "Intermodalità e trasporto combinato. Lineamenti teorici ed operativi", Quaderni della Rivista dei trasporti europei, Trieste

McAfee R.B., Glassman M., Honeycutt E.D. (2002) - "The effects of culture and human resource management policies on supply chain management", Journal of Business Logistics (Vol. 23 No. 1, pp. 1-18)

Mello J.E., Stank T.P. (2005) – "Linking firm culture and orientation to supply chain success", International Journal of Physical Distribution & Logistics Management (Vol. 35 No. 8, pp. 542-554)

Min S., Mentzer J.T., Ladd T. (2004) - "A market orientation in supply chain management", Department of Marketing, The University of Oklahoma, Norman

Morgan R.M., Hunt S.D (1994) - "The commitment-trust theory of relationship marketing", Journal of Marketing (Vol. 58 No. 3, pp. 20-38)

Motorola (2004) - "The opportunities for active RFID in container shipping"

Nassimbeni G. (2009) – "Il problema della vulnerabilità delle moderne reti internazionali", Logistica Management (Dicembre 2009, pp. 19-22)

Newman E., van Selm J. (2003) – "Refugees and Forced Displacement: International Security,
Human Vulnerability, and the State", United Nations University Press, Geneva.

Northland Insurance (2003) – "Vehicle & Cargo theft"

O'Hanlon M. (2002) - "Protecting the American Homeland", Brookings Institution Washington DC

Peck H. (2005) – "Drivers of supply chain vulnerability: an integrated frame work", International Journal of Physical Distribution & Logistics Management (Vol. 35, No. 4, pp. 210-232)

Peleg-Gillai B., Bhat G., Sept, L. (2006) - "Innovators in supply chain security: better security drives business value", The Manufacturing Innovation Series

Powell W.W. (1998) - "Learning from collaboration: knowledge and networks in the biotechnology and pharmaceutical industries", California Management Review (Vol. 40 No. 3, p. 228)

Purtell D. (2006) – "Is it safer?", Cargo Security International (Ottobre/Novembre 2006)

Purtell D., Rice J.B. (2007) – "Assessing cargo supply risk", Security Management Magazine Online

Quattroccolo F. (2011) – "Il treno è un giocattolo per ricchi? Riflessioni sul reale costo del trasporto su ferro", Ship2Shore (17/10/2011)

Quinn F.J. (2003), "Security matters", Supply Chain Management Review (Vol. 7 No. 4, pp. 38-45)

Rasmussen J., Vincente K.J. (2000) - "Proactive Risk Management in a Dynamic Society", Swedish Rescue Services Agency

Reason J. (1990) - "Human Error", Cambridge University Press, Cambridge

Rice J.B., Caniato F. - "Building a secure and resilient supply chain", Supply Chain Management Review (Settembre/ottobre 2003, pp. 22-33)

Rice J.B., Spayd P.W. (2005) - "Investing in supply chain security: collateral benefits", Special Report Series, IBM Center for The Business of Government

Russell D.M., Saldanha, J.P. (2003) - "Five tenets of security-aware logistics and supply chain operation", Transportation Journal (Vol. 42 No. 4, pp. 44-54)

Sambasivan M., Yen C.N. (2010) – "Strategic alliances in a manufacturing supply chain. Influence of organizational culture from the manufacturer's perspective", International Journal of Physical Distribution & Logistics Management (Vol. 40 No. 6, pp. 456-474)

Sarathy R. (2005) – "Terrorism, Security and the Global Supply Chain", International Trade and Logistics, Corporate Strategies and the Global Economy Conference, University of Le Havre

Sarathy R. (2006) – "Security and the Global Supply Chain" Transportation Journal (Vol. 45 No. 4, pp. 21-8)

Schein E. (1992) – "Organizational Culture and Leadership", Josey-Bass Publishers, San Francisco

Sheffi Y. (2001) - "Supply chain management under the threat of international terrorism", International Journal of Logistics Management (Vol. 12, No. 2, pp.1-11)

Sheffi Y. (2005) - "Weathering the storm", The business review for procurement leaders

Sheffi Y. (2005b) – "The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage", The MIT Press

Sheffi Y. (2005c) - "Preparing for the Big One", IEE Manufacturing Engineer (October/November 2005 ,pp. 12-16)

Sheffi Y., Caniato F., Rice J.B., Fleck J.M. (2003) – "Supply chain response to global terrorism: a situation scan", EurOMA POMS Joint International Conference, 17/6/2003, Cernobbio

Sheffi Y., Rice J. B. (2005) "Building the resilient enterprise", MIT Sloan Management review (Vol.40, N0.1, pp.40-49)

Shub A.N., Stonebraker P.W. (2009) – "The uman impact on SC: evaluating the importance of soft areas on integration and performance", Supply Chain Management: An International Journal (14/1/2009, pp. 31–40)

Siguaw J.A., Simpson P.M., Baker T.L. (1998) - "Effects of supplier market orientation on distributor market orientation and the channel relationship: the distributor perspective", Journal of Marketing (Vol. 62 No. 3, pp. 99-111)

Spekman R.E., Spear J., Kamauff, J. (2002) - "Supply chain competency: learning as a key component", Supply Chain Management (Vol. 7 No. 1, p. 41)

Strategic Forecasting Inc. (2006) – "Cargo theft: from silent crime to violent crime?", disponibile su www.stratfor.com

Strom K., Berzofsky M., Shook-Sa B., Barrick K., Daye C., Horstmann N., Kinsey S. (2010) – "The Private Security Industry: A Review of the Definitions, Available Data Sources, and Paths Moving Forward", Report of US Department of Justice

Stratfor inc.(2006) - "Cargo theft: from silent crime to violent crime?"

Talib F., Rahman Z., Qureshi M.N. (2011) – "A study of total quality management and supply chain management practices", International Journal of Productivity and Performance Management (Vol. 60 No. 3, pp. 268-288)

Tan K.C., Kannan K., Handfield R.B. (1998) - "Supply chain management: supplier performance and supplier performance", International Journal of Purchasing & Materials Management (Vol. 34 No. 3, pp. 2-9)

Thibault M., Brooks M.R., Button K.J. (2006) - "The response of the US maritime industry to the new container security initiatives", Transportation Journal (Vol. 45 No.1, pp. 5-15)

Tsang E.W.K. (1999) - "Internationalization as a learning process: Singapore MNCs in China", Academy of Management Executive (Vol. 13 No. 1, p. 91)

Tsiakouri M. (2008) – "Managing disruptions proactively in the supply chain", POMS 19th Annual Conference, 9-12/5/2008, California

Ueno A. (2008) - "Which managerial practices are contributory to service quality?", International Journal of Quality & Reliability Management (Vol. 25 No. 6, pp. 585-603)

Urciuoli L. (2009) – "Supply chain security. Mitigation measures and a logistics multi-layered framework", Department of Industrial Management and Logistics, Lund University

U.S. Custom and Border Protection (2006) – "Supply Chain Security best practice. C-TPAT"

van Oosterhout M., Veenstra A.W., Meijer G., Popal N., van den Berg J. (2006) – "Visibility Platforms for Enhancing supply cahin security: a case study in the port of Rotterdam", International Symposium on Maritime Safety, Security and Environmental Protection, Atene

Veenstra A.W. (2005) - "Supply chain security Definitions, PROTECT report D1.2", RSM Erasmus University Rotterdam

Werner S., Schuldt A., Daschkovska K. (2007) - "Agent-based container security systems: an interdisciplinary perspective", TZI University Brema, BIBA University Brema

Williams Z., Lueg J.E., LeMay S. (2008) – "Supply chain security: an overview and research agenda", The International Journal of Logistics Management (Vol. 19 No. 2, pp. 254-281)

Williams Z., Ponder N., Autry C.W. (2009) – "Supply chain security culture: measure development and validation", The International Journal of Logistics Management (Vol. 20 No. 2, pp. 243-260)

Willis H., Ortiz D (2004) – "Evaluating the security of the global containerized supply chain", Technical report of RAND Corporation

Wu S.J., Zhang D., Schroeder R.G. (2011) – "Customization of quality practices: the impact of quality culture", International Journal of Quality & Reliability Management (Vol. 28 No. 3, pp. 263-279)

Yin K.R. (1984) – "Case Study Research. Design and Methods", Sage Pubblications

Zairi M., Baidoun S. (2003) – "Understanding the Essentials of Total Quality Management: A Best Practice Approach", European Centre for TQM, Working Paper No 03/05, January 2003

Zsidisin G.A., Melnyk S.A., Ragatz, G.L. (2005) - "An institutional theory of business continuity planning for purchasing and supply chain management", International Journal of Production Research (Vol. 43 No. 16, pp. 3401-20)

Sitografia:

http://www.wikipedia.org

http://eur-lex.europa.eu/

http://www.businessdictionary.com

http://www.ilsole24ore.com/art/economia/2011-04-18/traffico-globale-container-riprende-204505.shtml?uuid=Aaq6f7PD

http://www.impresaitalia.info

http://www.ambrogio.it/

http://www.votg.de

http://www.terminaliitalia.it

http://www.terminalmortara.it/ita/

http://www.ewals.com/

http://www.sogemar.it/it/index.htm

http://www.rivaltalogistica.com/

http://www.fercam.com/it/

http://www.hupac.it/

http://www.hoyer-group.com/

http://www.mdbdesio.com/

http://www.marenzana.it/

http://www.bas.eu/Home.aspx

Altro materiale:

Brignoli G. - Slides "gestione del rischio", corso di Global Risk Management, Politecnico di Milano 2010

Melacini M. - Slide "sistemi di trasporto", corso di Modellazione dei Sistemi Logistici e Produttivi, Politecnico di Milano 2010