

IL PROBLEMA DELLA **VULNERABILITÀ** DELLE MODERNE RETI INTERAZIENDALI

di Guido Nassimbeni

• Guido Nassimbeni,
Università di Udine



Le moderne reti interaziendali sono decisamente più vulnerabili rispetto al passato: sono geograficamente più estese, coinvolgono attori più numerosi ed eterogenei, veicolano una molteplicità di contenuti materiali e immateriali. Si pone dunque il problema di governare questa complessità. Se quello del *risk management* è un filone ben consolidato in alcuni ambiti settoriali, la sua estensione all'ambito delle *operations* e della *supply chain* è relativamente recente. Questo intervento propone alcune considerazioni introduttive sul tema, utili per individuarne alcune declinazioni ed indirizzare approfondimenti successivi



1. LA CRESCENTE ARTICOLAZIONE E COMPLESSITÀ DELLA MODERNA SUPPLY CHAIN

“Una supply chain è una rete di risorse che svolge le funzioni di approvvigionamento dei materiali, e più in generale degli input di produzione, di trasformazione di questi in prodotti

intermedi e finiti, di distribuzione e consegna dei prodotti finiti ai clienti, e che è composta da imprese autonome che condividono finalità comuni” (Ganeshan e Harrison, 1999).

Questa definizione pone accento sull'interdipendenza degli attori che appartengono alla medesima *supply*

chain: repentine crisi insistenti su uno o più nodi inevitabilmente creano perturbazioni che possono destabilizzare il sistema nel suo complesso. Un elemento che negli ultimi anni ha acquisito una crescente importanza è dunque il fattore sicurezza. Alcuni eventi lo hanno portato prepotentemente alla ribalta: pensiamo

agli episodi terroristici di recente memoria, che hanno sollecitato alcuni governi ad investire massicciamente su questo fronte, incentivando la ricerca di tecnologie e strumenti di gestione a favore della *security* dei flussi di materiali, di persone e di informazioni. Pensiamo ancora al fenomeno SARS, che nel 2003 dalla Cina si è propagato in diversi Paesi del mondo, mettendo a nudo la vulnerabilità delle *supply chain* che collegano il Far East ai mercati occidentali. Ma a prescindere da questi eventi estemporanei, esistono motivazioni "strutturali" che giustificano la grande attualità del tema. Tra questi:

- la superiore complessità del prodotto/servizio associata a maggiori contenuti di innovazione tecnologica e di valore immateriale in esso incorporato. Questa complessità comporta il coinvolgimento di uno spettro ampio di attori, non solo distributori, fornitori o clienti, ma anche progettisti esterni, consulenti, erogatori di tecnologia, finanziatori. Una rete di stakeholders che richiede un presidio adeguato dei diversi snodi per preservare l'integrità dei flussi e il valore in essa trasportato.

- il crescente ricorso all'*outsourcing*. In mercati iper-competitivi come quelli attuali diventa fondamentale individuare un ristretto numero di competenze chiave sulle quali costruire il proprio vantaggio competitivo. Il ricorso a specialisti esterni a sostegno e complemento dei processi interni trasforma evidentemente

l'articolazione della rete di fornitura.

- l'estensione su base internazionale / globale delle attività aziendali. La mobilità transnazionale di capitali, informazioni, risorse umane, prodotti e servizi, incrementa la superficie di esposizione a possibili fattori di instabilità.

- l'adozione di logiche *lean* nella gestione dei flussi. Se in passato il sistema produttivo veniva isolato dalle perturbazioni di monte e di valle attraverso elementi di disaccoppiamento come le scorte, le logiche "snelle" orientano alla "fluidificazione" e alla velocizzazione di un flusso "in tiro" con il mercato. Da qui nasce la lotta sistematica alle scorte, la diminuzione della numerosità dei lotti, la ricerca dell'integrazione operativa tra attività interne od esterne. Ma da qui anche le

superiori esigenze di salvaguardia dei sistemi operativi.

Assistiamo pertanto a reti produttive, logistiche e commerciali più estese, articolate e complesse rispetto al passato. Reti dunque più esposte a rischi di *disruptions* e alle quali vengono richiesti superiori requisiti di sicurezza e resilienza.

2. "DISRUPTION". SICUREZZA E RESILIENZA

Il termine *disruption*, ricorrente nella letteratura non solo anglosassone sul tema, 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. Sheffi et al. (2003) distinguono le

“ Una *supply chain* è una rete di risorse che svolge le funzioni di approvvigionamento dei materiali, e più in generale degli *input* di produzione, di trasformazione di questi in prodotti intermedi e finiti, di distribuzione e consegna dei prodotti finiti ai clienti, e che è composta da imprese autonome che condividono finalità comuni” (Ganeshan e Harrison, 1999)

TABELLA 1 DISRUPTIONS E POSSIBILI AMBITI DI INTERVENTO (ADATTATA DA SHEFFI ET AL., 2003, E LEE E WOLFE, 2003).

AREA DEGLI APPROVVIGIONAMENTI	<ul style="list-style-type: none"> ■ Scelta del profilo, della numerosità e della localizzazione delle fonti di fornitura ■ Riprogettazione di prodotto e processo 	<ul style="list-style-type: none"> ■ Flessibilità dei contratti di fornitura ■ Politiche di gestione scorte
AREA DEL SISTEMA DEI TRASPORTI	<ul style="list-style-type: none"> ■ Collaborazione con provider ■ Modalità di trasporto molteplici 	<ul style="list-style-type: none"> ■ Molteplicità dei centri distributivi ■ Coinvolgimento del cliente
AREA DEL FLUSSO DEI MATERIALI	<ul style="list-style-type: none"> ■ Tracciabilità del prodotto ■ Controllo di prodotto e processo 	<ul style="list-style-type: none"> ■ Tracking delle merci ■ Verifiche ispettive
AREA DELLE INFRASTRUTTURE PRODUTTIVE	<ul style="list-style-type: none"> ■ Molteplicità dei siti produttivi ■ Accordi con fornitori di tecnologia e impianti 	<ul style="list-style-type: none"> ■ Infrastrutture produttive di back up
AREA DEI SISTEMI INFORMATIVI	<ul style="list-style-type: none"> ■ Misure di base ■ Assistenza di provider informatici 	<ul style="list-style-type: none"> ■ Creazione di dati di back up ■ Doc. Pr. sulla Sicurezza (DPS) ■ Disaster Recovery Plan
AREA DELLE RISORSE UMANE	<ul style="list-style-type: none"> ■ Piani di sostituzione ■ Reclutamento di personale idoneo 	<ul style="list-style-type: none"> ■ Cross training dei dipendenti ■ Flessibilità di utilizzo della forza lavoro

disruption in funzione del oggetto coinvolto:

- **Disruption della fornitura.**

Intervengono sulle attività di produzione degli input, bloccando o rallentando l'alimentazione delle unità di valle;

- **Disruption del sistema di trasporto.**

Intervengono sui vettori o sulla rete di trasporto;

- **Disruption del flusso materiali.**

Consistono nella violazione dell'integrità dei carichi e dei prodotti, con conseguente perdita o alterazione degli ordini e delle merci. Può essere dovuta a furto, a contaminazione o a manomissione;

- **Disruption delle infrastrutture produttive.**

Interrompono il normale funzionamento di impianti o macchinari, paralizzando la produzione;

- **Disruption del sistema informativo.**

Intervengono sul flusso di informazioni che accompagna quello dei materiali, bloccando o distorcendo la comunicazione tra le risorse umane e tecniche responsabili dei processi di trasformazione e trasporto;



8° Fiera internazionale specializzata per la distribuzione e per il flusso di materiali ed informazioni

2 - 4 Marzo 2010

Nuovo Centro Fieristico di Stoccarda, Germania

Varcate i confini Conquistate nuovi mercati



Il settore si incontra a Stoccarda
Oltre 700 espositori
Vi invitano a partecipare!

■ **Disruption** nelle **risorse umane**. Consistono nella indisponibilità temporanea o permanente di personale a presidio delle diverse attività.

La vulnerabilità di una rete inter-aziendale alle precedenti categorie di disruption è il risultato di due caratteristiche tra loro correlate ma che è opportuno distinguere:

■ la **sicurezza**, 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*. E' dunque la capacità di reagire con rapidità a fronte di instabilità della rete.

La prima è dunque una misura statica del rischio, la seconda cattura la capacità dinamica dell'impresa di recuperare rapidamente la condizione di regime. Pur esistendo un'area di sovrapposizione tra gli strumenti tecnologici e gestionali che insistono sulle due caratteristiche, la loro configurazione e il loro dimensionamento possono distinguersi. A titolo di esempio, i *firewall* di un sistema informativo

funzionalità dipende inoltre dall'esistenza di un disegno organizzativo chiaro e dalla polivalenza della risorse umana, a sua volta risultato di specifici canoni di reclutamento e percorsi professionali interfunzionali.

■ **(ri)configurazione dell'ambiente operativo**. Se la sicurezza del sistema operativo dipende dalle misure di prevenzione e controllo, la sua resilienza appare innanzitutto legata alla tipologia delle risorse produttive impiegate, e in particolare alla loro rapida riconfigurabilità, e alla disponibilità di risorse in eccesso: scorte, macchinari, impianti e installazioni che possono sostituire quelle paralizzate. Sistemi operativi che operano in prossimità della saturazione non dispongono evidentemente di gradi di libertà per fronteggiare imprevisti. Tuttavia, 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.

“ Assistiamo pertanto a reti produttive, logistiche e commerciali più estese, articolate e complesse rispetto al passato. Reti dunque più esposte a rischi di disruptions e alle quali vengono richiesti superiori requisiti di sicurezza e resilienza ”

prevedono attacchi virali indesiderati, come tali vigilano sulla sua sicurezza. Viceversa, il *back up* periodico del sistema può consentire una rapida rigenerazione delle funzionalità in caso di rotture, pertanto ne supporta la resilienza.

3. AREE DI INTERVENTO

Rispetto alle categorie di *disruption* sopra elencate, la tabella 1 individua possibili azioni di prevenzione o ripristino.

Le azioni sommariamente indicate in tabella individuano risposte che si muovono lungo queste principali direzioni:

■ **organizzazione**. Un efficace progetto per la salvaguardia della sicurezza prevede specifici piani di contingenza, cioè procedure e norme che orientino i comportamenti nelle situazioni crisi, e azioni formative basate su simulazioni ed esercitazioni tattiche. La capacità di restituire alle organizzazioni la piena

■ **(ri)configurazione del prodotto**. 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.

■ **(ri)configurazione del supply network**. La resilienza di una rete dipende non solo dal profilo dei suoi nodi e dei suoi collegamenti, ma anche dalla sua morfologia. Fonti di fornitura multiple, l'utilizzo di diversi vettori e modalità di trasporto, la disponibilità di centri di approvvigionamento, produzione e distribuzione alternativi tra loro, permettono di ridisegnare il percorso dei flussi in funzione della vischiosità che essi incontrano.

Queste direzioni di intervento non possono prescindere dalle opportunità offerte dallo sviluppo tecnologico. Pensiamo ad esempio ai moderni strumenti di tracking dell'ordine, come quelli che si avvalgono di tecnologie RFID, che consentono la rapida raccolta di informazioni su localizzazione e stato dell'ordine, con importanti conseguenze sulla sicurezza e sulle modalità di governo del flusso.

4. RISCHIO: UN PROBLEMA DI BILANCIAMENTO

Nel configurare il proprio sistema di sicurezza e resilienza, le organizzazioni devono fronteggiare una serie di scelte tra loro contrastanti (trade-off). Rielaborando il contributo di Sheffi (2003), le principali inconciliabilità ci sembrano le seguenti:

■ Ripetitività vs imprevedibilità.

L'utilizzo di risorse già sperimentate, il ricorso a relazioni consolidate, in generale la scelta di percorrere sentieri conosciuti riducono alcune potenziali sorgenti di instabilità. Inoltre, l'accumulazione di esperienza sui percorsi tradizionali favorisce le economie dinamiche, con un

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.** 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.

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.

Il conclusione, sicurezza e resilienza costano. Un costo che tende a crescere esponenzialmente in prossimità della soglia (puramente ideale) del rischio pari a zero. Il punto è allora quello di definire un valore di accettabilità del rischio, un valore cioè compatibile con i costi necessari per prevenirlo e intervenire sulle possibili emergenze.

5. CONCLUSIONI

Il fattore sicurezza e resilienza nelle catene produttive e logistiche è un tema ancora poco indagato nella letteratura scientifica e piuttosto distante dalla realtà di molte industrie. Questo ritardo trova due principali motivazioni. La prima è il costo che le soluzioni individuabili comportano. La seconda è la complessità degli interventi richiesti, associata alla loro dimensione sistemica. L'approccio con cui un'impresa può affrontare i rischi insistenti sulla propria supply chain deve essere strutturato, inter-disciplinare e deve naturalmente estendersi alle unità di monte o di valle. Gli aspetti inter-organizzativi e gestionali sono decisivi perché le cause di vulnerabilità spesso non risiedono in difetti o errori individuali, ma nella mancata interazione fra le molteplici parti coinvolte. Non è possibile, dunque, pensare di sviluppare strategie di prevenzione, controllo e ripristino efficaci senza organizzare sistematicamente il contributo di una pluralità di risorse, attori e discipline attorno al medesimo obiettivo. Lentamente e gradualmente, tuttavia, la consapevolezza sull'attualità di queste problematiche sta emergendo. □

“ Non è possibile, dunque, pensare di sviluppare strategie di prevenzione, controllo e ripristino efficaci senza organizzare sistematicamente il contributo di una pluralità di risorse, attori e discipline attorno al medesimo obiettivo ”

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 manomissione 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 e domestico vs estero.** 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

■ **Collaborazione vs. segretezza.** 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.

■ **Ridondanza di risorse vs "leaness".** E' questa la contrapposizione probabilmente più rilevante. Diverse tra le azioni enumerate nella precedente sezione fanno riferimento all'utilizzo di risorse in eccesso: impianti o macchinari produttivi,

Bibliografia

- Lee, H., Wolfe, M., "Supply Chain security without tears", *Supply Chain Management Review*, Vol. 7 No.1, pp.12-20, 2003.
- Rice, J., Caniato, F. "Supply Chain Response To Terrorism: Creating Resilient And Secure Supply Chains" *Supply Chain Response to Terrorism Project – Interim Report of Progress and Learning*, MIT Center for Transportation and Logistics, Massachusetts, 2003.
- Sheffi, Y. "Supply chain management under the threat of international terrorism: a situation scan", *The International Journal of Logistic Management*, Vol.12, num.2, pp. 1-11, 2003