Dal cyber al fisico: costruire l'Executive Awareness sul rischio cyber-fisico nelle organizzazioni complesse

Abstract

L'integrazione sempre più profonda tra tecnologie informatiche e asset operativi ha dato vita a un nuovo paradigma di minaccia: il rischio cyber-fisico. A differenza delle minacce informatiche tradizionali, limitate alla sottrazione di dati o all'interruzione di servizi digitali, gli attacchi ai sistemi cyber-fisici possono causare danni materiali diretti, interruzioni prolungate della catena cinematica e rischi concreti per l'incolumità umana. Nonostante la gravità di tali scenari, persiste spesso un pericoloso divario comunicativo tra i dipartimenti tecnici e i vertici aziendali.

L'obiettivo di questo intervento è definire un modello di Executive Awareness capace di trasformare la complessità tecnica in una narrazione strategica. Per ottenere il supporto della leadership, la sicurezza non deve più essere percepita come un mero centro di costo tecnologico, ma come un pilastro fondamentale della business continuity e della resilienza operativa. È necessario che il management comprenda che un'anomalia può oggi tradursi in un guasto meccanico o in un disastro ambientale.

Il documento analizza quattro pilastri fondamentali per una comunicazione efficace:

- dalla vulnerabilità all'impatto: tradurre concetti come exploit e malware in termini di ore di fermo macchina, danni reputazionali e impatto sul fatturato.
- L'integrazione IT-OT: spiegare come la protezione delle infrastrutture critiche richieda una governance olistica che abbatta i silos dipartimentali tra ingegneri e responsabili IT.
- Compliance e responsabilità: analizzare l'evoluzione delle normative internazionali, che sempre più spesso chiamano i dirigenti a rispondere personalmente della mancata adozione di misure di sicurezza adeguate.
- Il ROI della resilienza: dimostrare che l'investimento nella protezione degli asset fisici è un vantaggio competitivo che garantisce stabilità e fiducia nel mercato.

In conclusione, sensibilizzare il board significa passare da una gestione reattiva delle emergenze a una cultura della governance proattiva. Solo attraverso una comprensione chiara del rischio cyber-fisico, gli executive possono prendere decisioni informate, proteggendo non solo il patrimonio informativo, ma l'operatività industriale e l'integrità delle infrastrutture.

1. Introduzione

Negli ultimi anni, la trasformazione digitale dei processi industriali ha profondamente modificato il profilo di rischio delle organizzazioni complesse. La convergenza tra sistemi di Information Technology (IT) e quelli di Operational Technology (OT), inizialmente adottata per migliorare l'efficienza operativa, l'automazione e la visibilità dei processi, ha comportato un significativo ampliamento della superficie di attacco esposta a minacce informatiche [1], [2]. In tale contesto, il concetto di rischio cyber-fisico ha assunto una crescente rilevanza,

indicando la possibilità che un evento cyber produca conseguenze dirette e tangibili nel dominio fisico, con impatti sugli asset materiali, sulle operazioni industriali e sulla sicurezza delle persone.

A differenza degli scenari tradizionali di cybersecurity, storicamente focalizzati sulla compromissione della riservatezza, dell'integrità o della disponibilità dei dati, gli attacchi ai sistemi cyber-fisici introducono una scala di impatto significativamente diversa. Incidenti che coinvolgono sistemi di controllo industriale, infrastrutture critiche o ambienti OT possono infatti causare fermi produttivi prolungati, danni fisici agli impianti, interruzioni della supply chain e, nei casi più gravi, rischi concreti per la salute, la sicurezza e l'ambiente [3], [4]. Di conseguenza, il rischio cyber non può più essere considerato una minaccia puramente digitale, ma deve essere riconosciuto come un rischio operativo strategico per l'impresa.

Nonostante questo cambiamento di paradigma, molte organizzazioni faticano ancora a portare il rischio cyber-fisico all'attenzione dei livelli decisionali più alti. La sicurezza informatica è spesso percepita dal top management come una funzione tecnica o come un centro di costo, piuttosto che come un elemento abilitante della business continuity e della resilienza organizzativa [5], [6]. Tale disallineamento è in larga parte riconducibile a un persistente divario comunicativo tra le squadre tecniche e i vertici aziendali.

La letteratura evidenzia come questo divario derivi dall'utilizzo di linguaggi, metriche e modelli interpretativi differenti. I professionisti della sicurezza tendono a descrivere le minacce in termini di vulnerabilità, exploit e indicatori di compromissione, mentre il consiglio di amministrazione e il top management valutano il rischio principalmente sulla base di impatti economici, operativi, reputazionali e normativi [7], [8]. In assenza di una narrazione del rischio condivisa, le minacce cyber-fisiche risultano difficilmente comprensibili a livello strategico e, di conseguenza, difficilmente governabili in modo efficace. Il problema è ulteriormente aggravato dalla tradizionale separazione tra le funzioni IT e OT. Questi domini rispondono infatti a priorità differenti – flessibilità, scalabilità e protezione delle informazioni nel contesto IT; sicurezza fisica, affidabilità e continuità operativa nel contesto OT – generando silos che ostacolano una visione integrata del rischio [2], [9]. Tuttavia, la crescente interdipendenza tra sistemi digitali e processi fisici rende tale frammentazione sempre meno sostenibile e richiede l'adozione di modelli di governance trasversali e olistici.

Alla luce di queste considerazioni, il presente contributo affronta il tema della Executive Awareness sul rischio cyber-fisico, proponendo un framework concettuale finalizzato a tradurre la complessità tecnica in una narrazione strategica accessibile ai vertici aziendali. L'assunto di base è che la sicurezza dei sistemi cyber-fisici debba essere trattata come una componente centrale della governance d'impresa, al pari dei rischi finanziari, operativi e normativi, e non come una mera questione tecnologica [4], [6].

L'articolo sviluppa questa prospettiva attraverso l'analisi di quattro pilastri fondamentali: la traduzione delle vulnerabilità tecniche in impatti misurabili sul business, la necessità di una governance integrata IT-OT, il ruolo crescente della compliance e delle responsabilità manageriali, e il valore strategico della resilienza operativa come fonte di vantaggio competitivo nel lungo periodo. In tal modo, si intende dimostrare come una corretta sensibilizzazione del board rappresenti un prerequisito essenziale per il passaggio da una gestione reattiva degli incidenti a una governance proattiva del rischio cyber-fisico.

2. Dal cyber al fisico: il cambiamento del paradigma di rischio

L'evoluzione del rischio cyber-fisico rappresenta una discontinuità sostanziale rispetto ai modelli tradizionali di cybersecurity. Per lungo tempo, la sicurezza informatica è stata interpretata prevalentemente come una problematica legata alla protezione dei dati e dei sistemi informativi, con impatti riconducibili alla perdita di riservatezza, integrità o disponibilità delle informazioni. In questo paradigma, le conseguenze di un attacco erano principalmente di natura digitale e, sebbene potenzialmente rilevanti dal punto di vista economico o reputazionale, raramente producevano effetti diretti sul mondo fisico. La progressiva integrazione dei sistemi IT con le tecnologie OT ha tuttavia indebolito in modo significativo questa distinzione. I sistemi di controllo industriale, un tempo isolati e progettati per operare in ambienti chiusi, sono oggi sempre più interconnessi con le reti aziendali, con piattaforme cloud e con dispositivi di campo intelligenti. Questa convergenza, pur abilitando nuovi modelli operativi e di business, espone processi fisici critici a minacce originariamente circoscritte al dominio digitale [1], [2].

In tale contesto, il rischio cyber assume una dimensione cyber-fisica: un vettore di attacco informatico può innescare eventi che si manifestano direttamente a livello operativo, meccanico o ambientale. La compromissione di un sistema OT non si traduce soltanto in un malfunzionamento software, ma può alterare il comportamento di macchinari, impianti e infrastrutture, con effetti che includono danni materiali, interruzioni della produzione e pericoli per la sicurezza degli operatori. Di conseguenza, il confine tra sicurezza informatica e sicurezza fisica risulta essere sempre più sfumato [3], [4].

Un elemento distintivo del rischio cyber-fisico è la non linearità dell'impatto. Anche eventi apparentemente limitati, come una singola vulnerabilità o una configurazione errata, possono generare conseguenze sproporzionate se coinvolgono sistemi critici o processi a elevata interdipendenza. In questi scenari, l'effetto di un attacco non si esaurisce nel punto di compromissione, ma si propaga lungo la catena operativa, influenzando la continuità del servizio, la supply chain e, in taluni casi, l'ambiente esterno all'organizzazione.

Dal punto di vista gestionale, questo cambiamento di paradigma rende inadeguati gli approcci di valutazione del rischio basati esclusivamente su metriche tecniche o informatiche. La severità di un incidente cyber-fisico non può essere valutata solamente in termini di numero di sistemi compromessi o di dati esfiltrati, ma deve essere analizzata in relazione all'impatto sui processi core, sugli asset fisici e sugli stakeholder. Ciò implica una ridefinizione delle priorità di sicurezza, che devono essere allineate non solo agli obiettivi IT, ma anche e soprattutto agli obiettivi operativi e strategici dell'organizzazione.

Un ulteriore aspetto critico riguarda la diversa tolleranza al rischio tra i domini IT e OT. Mentre nei sistemi informativi è spesso accettabile interrompere temporaneamente un servizio per applicare una patch o mitigare una vulnerabilità, nei sistemi OT la priorità è garantire la sicurezza fisica, continuità e affidabilità nel processo. Questa asimmetria rende il rischio cyber-fisico particolarmente complesso da gestire, poiché impone compromessi tra esigenze di sicurezza informatica e requisiti operativi stringenti [2], [9]. Considerando queste caratteristiche, il rischio cyber-fisico non può più essere trattato come una semplice estensione della cybersecurity tradizionale. Esso richiede un approccio sistemico, capace di considerare le interdipendenze tra componenti digitali e fisiche e di valutare gli effetti di

un incidente lungo l'intero ciclo operativo. In questo senso, il rischio cyber-fisico rappresenta una categoria di rischio trasversale, che attraversa i confini funzionali dell'organizzazione e coinvolge direttamente la governance aziendale.
Per i vertici aziendali, comprendere questo cambiamento di paradigma è un passaggio fondamentale. La mancata consapevolezza della natura cyber-fisica del rischio conduce spesso a decisioni incomplete o ritardate, basate su una sottostima dell'impatto potenziale degli incidenti. Al contrario, riconoscere che un evento cyber può tradursi in un guasto meccanico, in un fermo produttivo o in un incidente ambientale consente di collocare la sicurezza all'interno di una visione più ampia di resilienza operativa e gestione del rischio d'impresa. La sezione successiva approfondisce come questa complessità possa essere resa comprensibile a livello direzionale, analizzando il primo pilastro del modello proposto: la traduzione delle vulnerabilità tecniche in impatti concreti sul business.

3. Dalla vulnerabilità tecnica all'impatto sul business

Uno dei principali ostacoli alla comprensione del rischio cyber-fisico a livello esecutivo risiede nelle modalità con cui tale rischio viene tradizionalmente rappresentato. I processi di gestione della cybersecurity fanno spesso riferimento a metriche e classificazioni di natura fortemente tecnica, quali score di vulnerabilità, livelli di severità o indicatori di compromissione. Sebbene tali strumenti siano indispensabili per le attività operative di sicurezza, risultano di difficile interpretazione per il top management e scarsamente efficaci nel supportare processi decisionali di natura strategica. Nel contesto dei sistemi cyber-fisici, questa limitazione assume un peso particolarmente rilevante. Una vulnerabilità tecnica, se analizzata esclusivamente in termini informatici, non riflette necessariamente l'effettiva esposizione dell'organizzazione al rischio. Al contrario, il suo impatto deve essere valutato in relazione ai processi operativi coinvolti e alle conseguenze potenzialmente generate lungo l'intera catena del valore. Studi recenti evidenziano come incidenti informatici che colpiscono ambienti industriali possano tradursi in costi estremamente elevati a causa di interruzioni operative, danni agli asset fisici e ripercussioni sulla supply chain [3], [10].
Rapporti empirici confermano che la componente di business disruption rappresenta una quota significativa del costo complessivo degli incidenti cyber. Il *Cost of a Data Breach Report* di IBM, realizzato in collaborazione con il Ponemon Institute, mostra come, nei settori industriali e manufatturieri, il downtime non pianificato e i ritardi nel ripristino incidano in modo sproporzionato sui costi totali dell'incidente rispetto alla sola perdita di dati [10]. In tali contesti, anche brevi interruzioni operative possono generare perdite economiche rilevanti e compromettere la capacità dell'organizzazione di rispettare obblighi contrattuali e livelli di servizio.
Per rendere il rischio cyber-fisico comprensibile e rilevante a livello direzionale, risulta pertanto necessario un cambio di prospettiva: dalla vulnerabilità all'impatto. In questo approccio, il rischio viene reinterpretato in termini di conseguenze sul business, come ore di fermo produzione, perdita di fatturato, aumento dei costi operativi o esposizione a sanzioni normative. Tale traduzione consente di spostare il focus dalla probabilità tecnica dell'attacco alla severità dell'impatto, rendendo il rischio leggibile in una logica di gestione d'impresa. Questa esperienza è particolarmente evidente nel dominio OT, dove la

disponibilità, l'affidabilità e la sicurezza fisica dei processi costituiscono requisiti primari. A differenza dei sistemi IT tradizionali, nei quali un arresto temporaneo può spesso essere gestito attraverso procedure di ripristino standard, nei sistemi industriali un'interruzione non pianificata può avere effetti immediati e duraturi. Secondo l'ENISA, gli attacchi ai sistemi di controllo industriali vengono sempre più frequentemente associati a interruzioni dei processi produttivi e a rischi per la sicurezza, rendendo il collegamento tra cyber risk e impatto operativo un elemento centrale nella valutazione del rischio [11]. Dal punto di vista della governance, la traduzione delle vulnerabilità tecniche in impatti sul business rappresenta un passaggio fondamentale per allineare la sicurezza agli obiettivi strategici. I vertici aziendali sono chiamati a decidere sulla base di criteri economici, operativi e reputazionali; presentare il rischio cyber-fisico in termini coerenti con tali criteri consente di ridurre il divario comunicativo tra funzioni tecniche e leadership. In questo senso, concetti come exploit o malware assumono significato nella misura in cui vengono collegati a scenari concreti di perdita operativa o compromissione aziendale [4], [6]. Un approccio strutturato a tale problematica è rappresentato dall'adozione della Business Impact Analysis (BIA) in chiave cyber-fisica. Il National Institute of Standards and Technology (NIST) sottolinea come la BIA consenta di collegare eventi di sicurezza informatica agli effetti sull'organizzazione nel suo complesso, supportando processi di prioritizzazione del rischio e di integrazione con l'Enterprise Risk Management [12]. Applicata ai contesti OT, tale analisi permette di identificare gli asset realmente critici e di valutare le vulnerabilità non solo in base alla probabilità di sfruttamento, ma soprattutto in base alla gravità delle conseguenze. In assenza di questa traduzione, le decisioni in materia di sicurezza rischiano di essere percepite come arbitrarie o scollegate dalle esigenze del business. Al contrario, quando il rischio cyber-fisico viene espresso in termini di continuità operativa, sostenibilità economica e protezione degli stakeholder, la sicurezza cessa di essere interpretata come un mero costo e viene riconosciuta come un investimento funzionale alla resilienza organizzativa. In tal senso, il World Economic Forum evidenzia come la capacità di collegare cyber risk e impatto operativo costituisca un elemento chiave per il coinvolgimento efficace del board e per decisioni informate sugli investimenti in sicurezza [13].
Alla luce di queste considerazioni, la capacità di trasformare vulnerabilità tecniche in una rappresentazione chiara dell'impatto sul business costituisce il primo pilastro del modello di Executive Awareness proposto. Essa permette di creare un linguaggio condiviso tra funzioni tecniche e vertici aziendali e rappresenta il punto di partenza per una governance efficace del rischio cyber-fisico. La sezione successiva approfondisce il secondo pilastro del modello, analizzando il ruolo della governance integrata IT-OT nella gestione di tali rischi.

4. Governance integrata IT-OT

L'evoluzione del rischio cyber-fisico è strettamente legata alla progressiva convergenza tra sistemi IT-OT, un processo che, pur generando significativi benefici operativi, ha introdotto nuove complessità nella gestione della sicurezza. Se, da un lato, l'integrazione tra i due domini consente una maggiore efficienza, visibilità e capacità decisionale in tempo reale, dall'altro determina una crescente interdipendenza tra sistemi digitali e processi fisici, ampliando la superficie di attacco e rendendo il rischio più difficile da isolare e contenere

[1], [2]. Tradizionalmente le funzioni IT e OT sono state gestite come ambiti distinti, caratterizzati da differenti obiettivi, priorità e modelli operativi. I sistemi IT sono orientati alla gestione delle informazioni e privilegiano requisiti quali riservatezza, integrità e disponibilità dei dati. Al contrario, i sistemi OT sono progettati per garantire la continuità e la sicurezza dei processi fisici, dove la priorità è rappresentata da affidabilità, sicurezza operativa e uptime continuo. Questa differenza di prospettiva ha storicamente giustificato una separazione organizzativa e tecnologica tra i due domini.

La crescente interconnessione tra IT e OT, accelerata dalle iniziative di digitalizzazione e dall'adozione di tecnologie industriali come IoT e piattaforme cloud, ha tuttavia reso tale separazione sempre meno sostenibile. Come evidenziato da diversi studi, la convergenza IT-OT rappresenta oggi uno dei principali fattori di aumento del rischio cyber-fisico, poiché espone sistemi critici, originariamente isolati, a minacce provenienti dal dominio digitale [1], [9]. In questo scenario, un attacco ai sistemi IT può propagarsi verso l'ambiente OT, compromettendo direttamente asset fisici e processi industriali. Un aspetto particolarmente critico riguarda la gestione della sicurezza in contesti caratterizzati da priorità divergenti. Nei sistemi IT, l'applicazione tempestiva di patch di sicurezza è considerata una pratica fondamentale per la riduzione del rischio; nei sistemi OT, al contrario, l'aggiornamento dei software può essere limitato o ritardato a causa della necessità di garantire la continuità operativa e la stabilità dei processi. Questa asimmetria genera una tensione strutturale tra esigenze di sicurezza e requisiti operativi, che non può essere risolta attraverso approcci puramente tecnici, ma richiede un allineamento a livello di governance [2], [9].

Alla luce di queste dinamiche, la gestione efficace del rischio cyber-fisico richiede il superamento dei tradizionali silos organizzativi e l'adozione di una governance integrata IT-OT. Tale approccio implica una visione olistica del rischio, in cui responsabilità, processi e decisioni di sicurezza vengono coordinati trasversalmente tra le diverse funzioni aziendali. In particolare, diventa essenziale definire in modo chiaro il perimetro di responsabilità e di ownership del rischio, evitando sovrapposizioni o zone grigie che possano compromettere l'efficacia delle misure di protezione. In questo contesto, il ruolo del top management e del board assume una rilevanza centrale. La letteratura evidenzia come la mancanza di integrazione tra IT e OT sia spesso attribuibile non a limiti tecnologici, ma a carenze di natura organizzativa e decisionale [3], [5]. L'assenza di una visione strategica unificata può portare a investimenti disallineati, a una sottostima delle interdipendenze tra sistemi e, in ultima analisi, a una maggiore esposizione a rischi sistemici. Al contrario, un approccio di governance integrata consente di allineare le strategie di sicurezza agli obiettivi di business, migliorando la capacità dell'organizzazione di prevenire, rilevare e gestire incidenti cyber-fisici. Un elemento chiave di tale approccio è rappresentato dall'integrazione tra cybersecurity e Enterprise Risk Management (ERM). La gestione del rischio cyber-fisico non può essere confinata alle funzioni tecniche, ma deve essere inclusa nel più ampio portafoglio dei rischi aziendali, consentendo al management di valutarne l'impatto in relazione ad altre categorie di rischio, come quelle finanziarie, operative e normative. In questa prospettiva, la sicurezza diventa un fattore abilitante della resilienza organizzativa e della continuità del business.

Dal punto di vista operativo, la governance integrata IT-OT si traduce nell'adozione di pratiche e strumenti capaci di favorire il coordinamento tra le diverse funzioni, quali la

definizione di policy condivise, la creazione di team multidisciplinari e l'implementazione di processi di reporting orientati al rischio. In particolare, la comunicazione tra i livelli tecnici e il top management assume un ruolo determinante nel garantire che le decisioni siano basate su una comprensione chiara e completa delle implicazioni del rischio cyber-fisico.
Infine, è importante sottolineare come la convergenza IT-OT non rappresenti solamente una sfida, ma anche un'opportunità. Se adeguatamente gestita, essa consente alle organizzazioni di sviluppare modelli operativi più efficienti e resilienti, capaci di sfruttare i benefici della digitalizzazione senza compromettere la sicurezza. Tuttavia, ciò richiede un cambiamento culturale oltre che tecnologico, in cui la collaborazione tra IT, OT e funzioni di governance diventa un elemento strutturale dell'organizzazione.
Alla luce di quanto proposto, la governance integrata IT-OT costituisce il secondo pilastro del modello di Executive Awareness proposto. Essa permette di superare la frammentazione organizzativa e di allineare la gestione del rischio cyber-fisico agli obiettivi strategici dell'impresa. Successivamente si analizzerà il terzo pilastro del modello, approfondendo il ruolo della compliance e della responsabilità manageriale nel contesto normativo emergente.

5. Compliance e responsabilità manageriali

L'evoluzione del rischio cyber-fisico non ha inciso unicamente sulle modalità operative delle organizzazioni, ma ha determinato anche un profondo cambiamento nel quadro normativo e nelle responsabilità attribuite al top management. Negli ultimi anni, si è assistito a una progressiva trasformazione della cybersecurity da ambito tecnico-specialistico a tema centrale di governance, con un corrispondente aumento delle aspettative nei confronti dei vertici aziendali in termini di supervisione, responsabilità decisionale e accountability [5], [6].
In questo nuovo contesto, la sicurezza dei sistemi informativi e delle infrastrutture operative non può più essere delegata esclusivamente alle funzioni tecniche. Le normative emergenti, sia a livello europeo sia internazionale, riconoscono esplicitamente il ruolo del management nella gestione del rischio cyber, richiedendo un coinvolgimento diretto nella definizione delle strategie di sicurezza, nell'assegnazione delle risorse e nella supervisione delle misure di mitigazione. Un esempio significativo è rappresentato dal rafforzamento dei requisiti normativi in materia di sicurezza delle infrastrutture critiche e resilienza operativa. Tali normative introducono obblighi stringenti in termini di gestione del rischio, reporting degli incidenti e adozione di misure preventive, attribuendo ai dirigenti responsabilità che vanno oltre la mera conformità tecnica. Come evidenziato da diversi studi, la mancata adozione di adeguate misure di sicurezza può esporre le organizzazioni non solo a sanzioni economiche, ma anche a conseguenze legali e reputazionali per il management [6].
Parallelamente, si osserva un'evoluzione del concetto di cybersecurity da requisito di compliance a componente integrante del dovere fiduciario degli amministratori. In questa prospettiva, il rischio cyber-fisico deve essere gestito con lo stesso livello di attenzione riservato ad altri rischi strategici, come quelli finanziari o operativi. Il board è chiamato non solo a essere informato sui rischi, ma anche a dimostrare di aver adottato processi adeguati per identificarli, valutarli e gestirli in modo sistematico [4], [5]. La crescente responsabilizzazione dei vertici aziendali è ulteriormente rafforzata dall'aumento della

complessità del contesto normativo, caratterizzato da una molteplicità di regolamenti e standard che richiedono coordinamento e integrazione. In questo scenario, la compliance non può essere interpretata come un insieme di adempimenti isolati, ma deve essere inserita in una strategia di governance del rischio più ampia e coerente. Ciò implica, tra l'altro, la necessità di allineare le politiche di sicurezza alle normative vigenti, garantire la tracciabilità delle decisioni e dimostrare la capacità dell'organizzazione di gestire efficacemente incidenti cyber-fisici. Un aspetto particolarmente rilevante riguarda il legame tra compliance e gestione della resilienza operativa. Le normative più recenti non si limitano a richiedere l'adozione di controlli di sicurezza, ma enfatizzano la capacità dell'organizzazione di prevenire, resistere e recuperare da eventi avversi. Questo approccio riflette un cambiamento di prospettiva: dalla protezione degli asset alla salvaguardia della continuità operativa e del valore aziendale. In tale ottica, la compliance diventa uno strumento per rafforzare la resilienza e per garantire la sostenibilità delle operazioni nel lungo periodo. Dal punto di vista della comunicazione, l'inquadramento del rischio cyber-fisico in termini di obblighi normativi e responsabilità manageriale rappresenta una potente leva per sensibilizzare il top management. Se nelle fasi precedenti l'attenzione era posta sull'impatto operativo ed economico degli incidenti, la dimensione della compliance introduce un ulteriore elemento di urgenza, legato alla possibilità di responsabilità personale e alla necessità di dimostrare un'adeguata governance del rischio.

Inoltre, il crescente interesse degli stakeholder – inclusi investitori, clienti e autorità di regolamentazione – nei confronti delle pratiche di sicurezza e resilienza aziendale contribuisce a rafforzare il ruolo della cybersecurity come fattore di fiducia e reputazione. Organizzazioni che non dimostrano un adeguato livello di maturità nella gestione del rischio cyber possono subire perdita di credibilità sul mercato, con conseguenze che si estendono ben oltre l'ambito strettamente tecnico.

In questo quadro, la compliance e la responsabilità manageriale rappresentano il terzo pilastro del modello di Executive Awareness proposto. Esse contribuiscono a rendere il rischio cyber-fisico non solo più comprensibile, ma anche concretamente rilevante per i vertici aziendali, stimolando un maggiore coinvolgimento nei processi decisionali e un allineamento più efficace tra strategie di sicurezza e obiettivi di business.

Il paragrafo successivo completa il modello analizzando il quarto pilastro, con particolare attenzione al ruolo della resilienza operativa e al valore strategico degli investimenti in sicurezza nei sistemi cyber-fisici.

6. Il valore strategico della resilienza operativa

Nel contesto dei sistemi cyber-fisici, la sicurezza non può più essere interpretata esclusivamente come un insieme di misure volte a prevenire o mitigare gli attacchi. La crescente complessità del panorama delle minacce e l'impossibilità di garantire una protezione assoluta rendono necessario un cambio di prospettiva: dalla sicurezza alla resilienza operativa. Quest'ultima si configura come la capacità dell'organizzazione di continuare a operare, adattarsi e recuperare rapidamente anche in presenza di incidenti significativi, preservando i propri obiettivi strategici [13]. A differenza degli approcci tradizionali, focalizzati prevalentemente sulla prevenzione, la resilienza riconosce che gli

attacchi cyber-fisici sono eventi inevitabili in ambienti altamente interconnessi. Di conseguenza, l'attenzione si sposta dalla semplice riduzione della probabilità di attacco alla gestione dell'impatto. In questo senso, la resilienza rappresenta la naturale evoluzione della cybersecurity, integrando capacità di risposta, adattamento e continuità operativa all'interno della strategia aziendale [13]. Nel dominio OT, questa prospettiva assume un'importanza ancora maggiore. La continuità dei processi industriali, la sicurezza degli impianti e la stabilità della produzione dipendono dalla capacità dell'organizzazione di reagire efficacemente a eventi avversi, minimizzando le interruzioni e garantendo il ripristino delle funzionalità critiche in tempi compatibili con le esigenze operative. In tali contesti, la resilienza non è un attributo accessorio, ma una componente essenziale del funzionamento stesso dell'impresa [1], [9]. Dal punto di vista strategico, la resilienza operativa consente di superare la tradizionale percezione della sicurezza come centro di costo. Se intesi esclusivamente come spesa, gli investimenti in cybersecurity tendono a essere sottovalutati o rinviati. Tuttavia, quando la sicurezza viene inquadrata come strumento per proteggere la continuità operativa, il valore aziendale e la fiducia degli stakeholder, essa assume una dimensione pienamente strategica [6], [13]. In questo senso, il concetto di ritorno dell'investimento (ROI) nella sicurezza non può essere misurato unicamente in termini di incidenti evitati, ma deve includere anche il valore della stabilità operativa e della capacità di risposta. Numerosi studi evidenziano come organizzazioni dotate di elevate capacità di resilienza siano in grado di ridurre significativamente l'impatto degli incidenti, sia in termini economici sia operativi. La rapidità di rilevazione, la capacità di contenimento e l'efficacia delle procedure di ripristino rappresentano fattori determinanti nel limitare le perdite e nel garantire la continuità del business [10], [12]. In questo quadro, l'investimento in resilienza si traduce in una riduzione del rischio complessivo e in una maggiore prevedibilità delle performance aziendali. Un ulteriore elemento di valore riguarda la dimensione reputazionale. In un contesto in cui clienti, partner e investitori attribuiscono crescente importanza alla capacità delle organizzazioni di gestire il rischio e garantire la continuità dei servizi, la resilienza diventa un fattore competitivo. Organizzazioni percepite come robuste e affidabili sono in grado di mantenere la fiducia del mercato anche in presenza di eventi avversi, rafforzando la propria posizione nel lungo periodo [4], [13]. Dal punto di vista della governance, la resilienza operativa richiede un approccio integrato che coinvolga l'intera organizzazione. Non si tratta di una funzione esclusivamente tecnica, ma di una capacità trasversale che richiede coordinamento tra sicurezza, operations, risk management e vertici aziendali. In questo senso, la resilienza rappresenta il punto di incontro tra le diverse dimensioni analizzate nelle sezioni precedenti: impatto sul business, governance IT-OT e compliance [5], [6]. Un approccio efficace alla resilienza cyber-fisica si basa su alcuni elementi chiave: la definizione delle priorità operative (identificazione degli asset critici), la pianificazione dei processi di risposta agli incidenti, l'esecuzione di esercitazioni e simulazioni (tabletop exercise) e la capacità di apprendere dagli eventi per migliorare continuamente i processi. Questi strumenti permettono di trasformare la gestione degli incidenti da attività reattiva a processo strutturato e integrato nella strategia aziendale [12].
In questo quadro, il ruolo del top management è determinante. La resilienza operativa deve essere promossa a livello strategico, integrata nei processi decisionali e supportata da investimenti adeguati. Senza una chiara visione da parte della leadership, il rischio è che le

iniziative di sicurezza rimangano frammentate e incapaci di produrre un reale aumento della capacità di risposta dell'organizzazione [5].
In questo contesto, la resilienza operativa rappresenta il quarto e conclusivo pilastro del modello di Executive Awareness. Essa segna il passaggio da un approccio difensivo della sicurezza a una prospettiva proattiva orientata alla continuità operativa e alla creazione di valore [13]. Integrata nei processi di governance aziendale, consente alle organizzazioni di affrontare in modo più efficace i rischi cyber-fisici, riducendone l'impatto e migliorando la capacità complessiva di risposta. Dunque, le vulnerabilità non sono più considerate esclusivamente come punti di debolezza, ma come elementi da gestire strategicamente, in grado di trasformarsi, se correttamente governati, in leve di rafforzamento competitivo [6], [13].

7. Un modello di Executive Awareness per il rischio cyber-fisico

La transizione da una gestione puramente tecnica della sicurezza a una governance strategica del rischio cyber-fisico richiede l'adozione di un framework operativo strutturato. Non è infatti sufficiente incrementare la frequenza dei flussi informativi verso il consiglio di amministrazione; è necessario intervenire sulla natura stessa delle informazioni trasmesse, affinché esse diventino strumenti di supporto alle decisioni strategiche e non semplici dati tecnici difficilmente interpretabili. Il modello di Executive Awareness proposto si sviluppa lungo tre direttrici principali, finalizzate a trasformare la complessità tecnica del rischio in leve decisionali utilizzabili dal top management: la quantificazione finanziaria del rischio, l'adozione di metriche di resilienza condivise e lo sviluppo di capacità decisionali tramite apprendimento esperienziale.
Il primo elemento riguarda il superamento delle tradizionali metodologie qualitative di valutazione del rischio, spesso basate su scale ordinali o rappresentazioni cromatiche che risultano poco significative per il board. In alternativa, il modello propone l'adozione di approcci di Cyber Risk Quantification (CRQ), in grado di integrare i risultati della Business Impact Analysis (BIA) con modelli quantitativi di stima delle perdite economiche. In un contesto cyber-fisico, questa prospettiva comporta la mappatura delle interdipendenze tra asset digitali e output industriali, rendendo esplicito il legame tra vulnerabilità logiche e conseguenze operative. In questo modo, il rischio non viene più rappresentato attraverso indicatori tecnici, ma mediante scenari di perdita economica espressi in termini monetari, includendo componenti quali il costo del downtime non pianificato, la sostituzione o il danneggiamento di asset fisici e gli impatti derivanti da responsabilità civile e ambientale. Tale approccio consente di integrare pienamente il rischio cyber-fisico nei processi di Enterprise Risk Management (ERM), rendendolo comparabile con altre categorie di rischio aziendale e supportando decisioni basate su criteri di costo-beneficio [12].
Accanto alla quantificazione del rischio, il modello prevede una profonda revisione delle metriche utilizzate per il reporting direzionale. I flussi informativi indirizzati al top management devono essere depurati da indicatori puramente operativi, come il numero di vulnerabilità rilevate o di attacchi bloccati, per concentrarsi su indicatori chiave di rischio e di performance orientati alla continuità operativa. In questo senso, l'attenzione si sposta verso metriche quali il livello di segregazione tra ambienti IT e OT, la capacità di rilevazione

tempestiva degli incidenti (Mean Time to Detect) e l'efficacia dei processi di ripristino (Mean Time to Recover). L'introduzione di indicatori sintetici di resilienza consente di fornire al board una rappresentazione chiara e comparabile dello stato di salute dell'organizzazione, favorendo un linguaggio condiviso tra funzioni tecniche e vertici aziendali. Questo tipo di approccio si inserisce in una più ampia evoluzione della cybersecurity verso una dimensione strategica, in cui la resilienza operativa diventa parametro centrale di valutazione del rischio e della capacità organizzativa [13].

Il terzo elemento del modello riguarda lo sviluppo della consapevolezza esecutiva attraverso strumenti di apprendimento esperienziale. In particolare, l'introduzione sistematica di esercitazioni di simulazione, come i tabletop exercises, consente ai membri del board e ai responsabili delle crisi di confrontarsi con scenari realistici di incidente cyber-fisico. A differenza delle esercitazioni tecniche, tali simulazioni non mirano a testare competenze specialistiche, ma a supportare i processi decisionali in condizioni di incertezza, pressione temporale e incompletezza delle informazioni. Gli scenari proposti includono eventi ad alto impatto, quali interruzioni della supply chain, manipolazioni malevole di sistemi di controllo industriale o incidenti con implicazioni ambientali e reputazionali, costringendo il management a valutare le conseguenze strategiche delle proprie decisioni.

L'esperienza dimostra come l'immersione guidata in contesti simulati rappresenti uno degli strumenti più efficaci per trasformare la percezione della cybersecurity da problema tecnico a tema centrale di governance. Attraverso tali esercitazioni, il top management acquisisce una comprensione diretta delle implicazioni operative, legali e reputazionali del rischio cyber-fisico, sviluppando una maggiore capacità di risposta coordinata e consapevole. In questo modo, la sicurezza viene progressivamente integrata nei processi decisionali strategici, contribuendo a rafforzare la resilienza complessiva dell'organizzazione e ad allineare le strategie di protezione agli obiettivi di business [5], [13].

8. Conclusioni

La crescente interconnessione che caratterizza l'era dell'Industria 4.0 e della transizione digitale ha reso ormai superati i paradigmi tradizionali della sicurezza. Come evidenziato nel corso di questo contributo, il rischio cyber non può più essere confinato a una dimensione puramente virtuale, né considerato un ambito di esclusiva competenza dei dipartimenti IT. L'emergere del rischio cyber-fisico richiede un profondo cambiamento di prospettiva, tanto sul piano concettuale quanto su quello gestionale: in un contesto in cui un'alterazione digitale può produrre effetti materiali, la sicurezza informatica diventa un elemento imprescindibile per la tutela degli asset fisici, della continuità operativa e della sicurezza delle persone.

In questo scenario, la costruzione di una solida Executive Awareness rappresenta il fattore abilitante per governare tale complessità all'interno delle organizzazioni. Il passaggio da una gestione reattiva delle emergenze a un approccio proattivo e strutturato alla governance del rischio si fonda su quattro direttrici fondamentali che coinvolgono direttamente il vertice aziendale.

In primo luogo, è necessario colmare il divario comunicativo tra funzioni tecniche e management. Attraverso strumenti di quantificazione del rischio, come la Cyber Risk

Quantification (CRQ) e la Business Impact Analysis, le vulnerabilità devono essere tradotte in impatti economici concreti — quali fermo macchina, perdita di fatturato o esposizione a sanzioni — in modo da rendere il rischio comprensibile e rilevante per il Board.
In secondo luogo, si impone il superamento dei silos organizzativi. La convergenza tecnologica tra IT e OT deve essere accompagnata da una convergenza a livello di governance, fondata su responsabilità condivise e su una visione integrata del rischio. Solo in questo modo è possibile rispondere efficacemente alle tensioni tra esigenze di sicurezza informatica e requisiti di continuità operativa.
Un terzo elemento riguarda la crescente centralità della responsabilità manageriale. L'evoluzione del quadro normativo internazionale sta progressivamente trasformando la cybersecurity in un dovere fiduciario degli amministratori, attribuendo loro responsabilità dirette nella supervisione e nella gestione del rischio. Questo cambiamento rafforza il ruolo del top management nella definizione delle strategie di sicurezza e nella protezione del valore aziendale.
Infine, la resilienza operativa emerge come una leva strategica fondamentale. Gli investimenti nella sicurezza dei sistemi cyber-fisici non possono più essere interpretati come semplici costi, ma devono essere considerati elementi chiave per garantire stabilità, continuità e fiducia nel mercato. In un contesto caratterizzato da elevata volatilità e interdipendenza, la capacità di assorbire e gestire un incidente cyber rappresenta un fattore distintivo di competitività.
In ultima analisi, sviluppare un modello strutturato di Executive Awareness non significa trasformare i decisori aziendali in esperti tecnici, ma renderli capaci di integrare il rischio cyber-fisico nei processi decisionali strategici. Solo quando la sicurezza dei sistemi operativi e delle infrastrutture industriali sarà pienamente incorporata nella cultura della governance d'impresa, le organizzazioni potranno affrontare la trasformazione digitale non come una fonte di fragilità, ma come un'opportunità di sviluppo solido, sostenibile e resiliente.

References

[1] KPMG, 2025, *IT/OT Cybersecurity Convergence Framework. Bridging IT and OT: Enhancing Security and Efficiency through Convergence*, KPMG International, https://assets.kpmg.com/content/dam/kpmg/de/pdf/Themen/2025/04/kpmg-it-ot-cyber-convergence-framework.pdf

[2] *Navigating IT OT Convergence: A Strategic Guide to Security and Risk*, 2024, https://www.isc2.org/Insights/2024/08/IT-OT-Convergence

[3] Cusimano J., 2025, *What is the board's role in cyber-risk management in OT environments?*, https://www.darkreading.com/cyber-risk/board-role-cyber-risk-management-ot-environments

[4] McKinsey & Company, 2024, *A board-level view of cyber resilience*, Risk & Resilience Practice, file:///C:/Users/Acer/Downloads/a-board-level-view-of-cyber-resilience.pdf

[5] PWC, Governance Insight Center, 2025, *The board's role in overseeing cybersecurity*, https://www.pwc.com/us/en/services/governance-insights-center/library/assets/pwc-2026-cybersecurity-oversight.pdf

[6] Thales, 2025, *The next outage is preventable: board accountability for cyber risk*, https://www.thalesgroup.com/sites/default/files/2026-04/Board%20Governance%20for%20Cybersecurity%20White%20Paper.pdf

[7] National Cyber Security Centre, 2024, *Engaging with Boards to improve the management of cyber security risk*, https://www.ncsc.gov.uk/files/NCSC-Board-level-cyber-discussions-communicating-clearly.pdf

[8] Kappel R., 2026, *Communicating Cyber Risk to the Board: Executive Reporting Best Practices*, https://www.centraleyes.com/communicating-cyber-risk-to-the-board-executive-reporting/

[9] Diamond D., 2025, *IT/OT Convergence: an Era of Interconnected Risk and Reward*, https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/an-era-of-interconnected-risk-and-reward

[10] IBM Security, 2025, *Cost of a Data Breach Report*, IBM Corporation, https://www.ibm.com/reports/data-breach

[11] European Union Agency for Cybersecurity - ENISA, 2025, *ENISA Threat Landscape 2025*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

[12] Quinn S. et Al., 2025, *Using Business Impact Analysis to Inform Risk Prioritization and Response*, National Institute of Standards and Technology (NIST), https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8286D-upd1.pdf

[13] Blassiau C. et Al., 2026, *Why cybersecurity is now a strategic imperative for business growth, trust and resilience*, World Economic Forum, https://www.weforum.org/stories/2026/03/cybersecurity-strategic-imperative-growth-resilience/