Gestione del rischio cyber, business continuity e crisis management

Cambi di paradigma in un contesto di multirischio: una *War Room* come architettura integrata di resilienza operativa in un contesto di multirischio e normativa *risk-based* e *resilience-based*.

Autore: Federica Maria Rita Livelli

Sommario

Executive Summary

Il panorama del rischio cyber, operativo e normativo sta attraversando una trasformazione profonda e irreversibile. Le organizzazioni si trovano oggi a dover fronteggiare non più i singoli eventi avversi, ma sistemi di rischio interconnessi, nei quali un incidente informatico può innescare - a cascata - interruzioni operative, danni reputazionali, sanzioni regolamentari e perdite finanziarie di portata sistemica.

La gestione tradizionale del rischio - basata su approcci compartimentati, piani di *business continuity* aggiornati con cadenza annuale e strategie di risposta calibrate su scenari storici - ha mostrato limiti strutturali evidenti.

È in atto un cambio di paradigma che ridefinisce le responsabilità dei risk manager, con particolare attenzione a **cinque aree critiche**, quali:

- l'**evoluzione delle minacce cyber** e la loro crescente sofisticazione sistemica;
- le **ragioni strutturali** per cui le organizzazioni falliscono nella gestione delle crisi;
- il **gap tra conformità normativa e reale capacità di risposta**;
- la riconfigurazione del perimetro del rischio nella **supply chain**;
- l'impatto delle **nuove normative europee** - NIS2, DORA, CRA e CER - sull'architettura della resilienza operativa.

Inoltre, il passaggio da un approccio reattivo a un'architettura integrata di resilienza richiede un modello operativo radicalmente nuovo. **Al centro di questo modello si trova la *War Room***: un'unità di comando e di coordinamento che integra competenze tecniche, legali, reputazionali e decisionali sotto un'unica regia, capace di ridurre la durata della crisi, limitarne gli impatti e ristabilire rapidamente continuità operativa.

Di fatto, la *War Room* non è un luogo fisico, ma un sistema adattivo in cui *crisis management*, coordinamento operativo e trasferimento intelligente del rischio diventano un'unica architettura organizzativa.

I dati del panorama attuale confermano l'urgenza di questa transizione:

13.800 MLD **Costo globale cybercrime** Stima entro il 2028 (miliardi di dollari)	**62% degli attacchi via supply chain** Principale vettore di compromissione	**Solo il 23% delle organizzazioni ripristino in 72h** Organizzazioni che recuperano entro 3 giorni da un incidente grave

Di fronte a questi numeri, il cambiamento non è più una scelta: è una necessità di sopravvivenza organizzativa. Costruire una *War Room* efficace e trasformarla in un'architettura permanente di resilienza è il vantaggio competitivo che separerà le organizzazioni capaci di affrontare le crisi da quelle destinate a subirle.

1.Il contesto: uno scenario del rischio in profonda evoluzione

Ci troviamo in un vero e proprio "*digital far west*", come definito da Clusit, in cui le organizzazioni devono dimostrare di essere in grado di gestire la cosiddetta "imprevedibile certezza del rischio cyber" in continua evoluzione e sempre più sistemico.

1.1 La convergenza delle crisi: dal rischio singolo al sistema di rischio

La gestione del rischio da parte delle organizzazioni, fino a pochi anni fa, poteva ancora seguire una logica modulare: il rischio informatico era presidio dell'IT; il rischio operativo era gestito dall'area *operations*; la *business continuity* era un piano nel cassetto da aggiornare ogni anno; la copertura assicurativa era una polizza rinnovata quasi automaticamente. Un approccio compartimentato che rifletteva una realtà nella quale i rischi, pur correlati, potevano essere ragionevolmente trattati in modo separato.

Oggi, tale realtà non esiste più. La trasformazione digitale ha "dissolto" le barriere tra le funzioni aziendali, creando un tessuto connettivo e vasi comunicanti fatto di API, cloud, SaaS e fornitori terzi che rende ogni sistema sempre più interconnesso e dipendente dagli altri.
Un *ransomware* che colpisce un fornitore di software, un'interruzione di un *hyperscaler cloud*, una *vulnerabilità zero-day* in un componente *open-source* ampiamente utilizzato può propagarsi attraverso centinaia di organizzazioni in poche ore, con effetti a cascata difficilmente contenibili.

Siamo di fronte a quello che gli analisti definiscono "rischio sistemico digitale" o "rischio di concentrazione tecnologica", emerso con chiarezza in alcuni eventi emblematici degli ultimi anni, quali il caso CrowdStrike del luglio 2024: un aggiornamento difettoso di un software di sicurezza ha causato l'interruzione di 8,5 milioni di sistemi Windows in tutto il mondo, bloccando aeroporti, ospedali, banche e servizi di emergenza. L'evento ha dimostrato con brutalità che l'interconnessione trasforma eventi locali in *disruption* globali e che l'affidabilità di un sistema complesso non è la somma delle affidabilità dei suoi componenti.

1.2 L'escalation delle minacce cyber: sofisticazione, persistenza, geopolitica

Il panorama delle minacce cyber ha subito una trasformazione qualitativa negli ultimi cinque anni. Non si tratta solo di un aumento quantitativo degli attacchi, ma di un salto di complessità in termini di tattiche, di tecniche e di procedure dei cyber criminali. Quattro tendenze meritano un'attenzione specifica e, precisamente:

1. **Professionalizzazione –** La professionalizzazione del crimine informatico attraverso il modello *Ransomware-as-a-Service (RaaS)*, che ha "democratizzato" la capacità offensiva, consentendo anche ad attori con competenze tecniche limitate di condurre campagne sofisticate, acquistando kit già pronti sul dark web.
2. **Ibridizzazione -** La crescente ibridazione tra criminalità organizzata e attori *state-sponsored* con gruppi che operano in zone grigie, dove interesse economico e interesse geopolitico si sovrappongono, rendendo difficile sia l'attribuzione sia la risposta diplomatica.

3. **AI come amplificatore -** L'uso dell'AI come amplificatore sia delle capacità offensive (i.e. phishing ultra-personalizzato, generazione automatica di *malware*, elusione dei sistemi di rilevamento) sia di quelle difensive (i.e. SIEM di nuova generazione e *threat intelligence* automatizzata).
4. ***Supply chain* -** Il targeting sistematico della supply chain come vettore di accesso preferenziale: attaccare un fornitore di software o di servizi permette di compromettere simultaneamente centinaia di organizzazioni, a valle.

A questi fattori si aggiunge la dimensione geopolitica: il conflitto in Ucraina-Russia ed ultimamente quello USA-Iran-Israele hanno accelerato l'uso di *cyber-weapon* come strumento di guerra ibrida, con effetti di *spillover* su organizzazioni private in Paesi terzi.

Inoltre, le tensioni tra le grandi potenze si proiettano nel cyberspazio come campo di competizione strategica, mentre le infrastrutture critiche – i.e. energia, trasporti, telecomunicazioni, finanza, spazio, ecc. - sono diventate teatri di operazioni di *intelligence* e sabotaggio digitale.

1.3 Il cambio normativo: da *compliance* a resilienza

Il legislatore europeo ha abbandonato l'approccio prescrittivo in favore di un approccio *risk-based* e *resilience-based*, nel quale l'organizzazione deve dimostrare non solo di aver implementato determinate misure, ma di **saper gestire il rischio in modo proporzionato e di poter mantenere — o ripristinare rapidamente — le proprie funzioni critiche in caso di interruzione**. Un cambio di paradigma impegnativo dato che richiede una maturità organizzativa e una capacità di valutazione del rischio che molte organizzazioni non hanno ancora sviluppato.

NIS2, DORA, il Cyber Resilience Act e la Direttiva CER (Critical Entities Resilience) convergono verso questa logica, costruendo un framework europeo della resilienza digitale che allinea gli incentivi dei regolatori con le necessità operative delle organizzazioni.
Di fatto, la compliance diventa il piano di partenza, non il punto di arrivo.

2. Perché le organizzazioni falliscono nella gestione delle crisi

Le organizzazioni di medio-grande dimensione dispongono, generalmente, di un *Business Continuity Plan (BCP)*, di un *Disaster Recovery Plan (DRP)*, oltre a un *Crisis Management Plan (CMP)*, periodicamente testati attraverso esercitazioni *tabletop* o simulazioni. **Eppure, quando la crisi reale arriva, le organizzazioni falliscono molto frequentemente nella gestione**.

Perché ciò accade? La risposta non sta nella qualità tecnica dei piani, ma in una serie di presupposti impliciti che i piani contengono e che la realtà sistematicamente viola. Il presupposto più pervasivo - e più insidioso - è quello della crisi come evento singolo e delimitato: un incidente con inizio, sviluppo e fine prevedibili, gestibile attraverso protocolli prestabiliti. La realtà delle crisi contemporanee è radicalmente diversa.

2.1 Le caratteristiche delle crisi cyber contemporanee

Gli incidenti cyber, oggi, si caratterizzano per:

- **Ambiguità iniziale** (i.e. non è chiaro cosa stia succedendo)
- **Escalation non lineare** (i.e. l'evento si espande in modi imprevedibili attraverso sistemi interconnessi)
- **Compressione del tempo decisionale** (i.e. le finestre di azione efficace si misurano in ore o minuti)
- **Contestualità** (i.e. la crisi si manifesta mentre l'organizzazione è impegnata nelle normali attività operative, creando conflitti di priorità).

Di fatto, **tutti questi elementi combinati producono un contesto radicalmente diverso da quello simulato nelle esercitazioni**, con il risultato che le competenze e i comportamenti addestrati non si trasferiscono automaticamente.

2.2 I fattori organizzativi del fallimento

È doveroso evidenziare che, al di là dei limiti dei piani, esistono fattori organizzativi strutturali che compromettono sistematicamente la capacità di risposta alla crisi. La ricerca accademica e l'analisi post-incidente convergono su sei dimensioni critiche e, precisamente:

1. **Frammentazione del comando** - In molte organizzazioni, la crisi cyber si trova all'incrocio tra le funzioni IT, Sicurezza, Legal, Comunicazione, Operations e Top Management, senza una chiara definizione di chi ha l'autorità decisionale in ogni fase. Pertanto, tale ambiguità produce paralisi: ognuno aspetta che decida qualcun altro; le riunioni si moltiplicano senza produrre decisioni; il tempo scorre favorendo l'attaccante.
2. **Sovraccarico cognitivo e stress decisionale** - La risposta a un incidente grave genera un flusso di informazioni – i.e. alert tecnici, log di sistema, comunicazioni interne, richieste dei media, domande degli stakeholder - che supera rapidamente la capacità di elaborazione degli individui e dei team. Ne consegue che, in assenza di sistemi di triage informativo e di protocolli di escalation consolidati, il rischio di decisioni errate o di non-decisioni è altissimo.
3. **Dipendenza da tecnologie compromesse** – È doveroso evidenziare che, frequentemente, i sistemi di comunicazione di crisi, i sistemi di ticketing degli incidenti, le piattaforme di collaborazione interna sono spesso ospitati sulle stesse infrastrutture che l'attaccante ha compromesso. Pertanto, un'organizzazione, colpita da ransomware e che usa Microsoft Teams per coordinare la risposta, ad esempio, può scoprire troppo tardi che Teams è inaccessibile.
4. **Gap nella comunicazione della crisi** - La gestione tecnica di un incidente cyber è una cosa; la comunicazione verso clienti, partner, autorità di vigilanza, media e mercati finanziari è un'altra. Tali competenze difficilmente coesistono nelle stesse persone e, raramente, sono adeguatamente coordinate.
5. **Mancanza di resilienza finanziaria immediata** - Le crisi generano costi improvvisi e urgenti – i.e. *forensics investigation*, *incident response* esterni, comunicazioni di crisi, rimpiazzo di hardware, potenziali risarcimenti - che possono creare tensioni finanziarie acute se

l'organizzazione non ha predefinito previamente i meccanismi di allocazione e le modalità di accesso alle risorse.

6. ***Normalcy bias*** **–** Si tratta di un aspetto sottile, che consiste nella tendenza cognitiva a sottostimare la gravità di eventi anomali e a cercare interpretazioni rassicuranti. Di fatto, nelle prime ore di un incidente, spesso, si tende a pensare che, probabilmente, si tratti di un falso positivo e si possa risolvere senza allertare il Top Management, in modo da capire meglio prima di attivare il piano di crisi. Tale ritardo nell'attivazione, in molti casi, ha la capacità di determinare la gravità finale dell'incidente.

2.3 Tempistiche di risposta agli incidenti cyber

È interessante notare che, nel 2025, il tempo medio per attivare le procedure di gestione delle crisi si è ridotto significativamente a causa delle pressioni normative, con molte organizzazioni che puntano ad attivare i piani di risposta entro 60 minuti dal rilevamento.

Tuttavia, il **tempo medio per rilevare e contenere completamente una violazione** rimane elevato, stimato a **241 giorni nel 2025** (181 giorni per l'identificazione, 60 giorni per il contenimento), sebbene ciò rappresenti una risposta più rapida rispetto agli anni precedenti, secondo quanto si evince dal **rapporto IBM "Cost of data breach 2025"** sui costi delle violazioni dei dati e dal **rapporto Verizon 2025** sulle indagini sulle violazioni dei dati. Ciò è principalmente dovuto a sistemi di sicurezza avanzati basati sull'AI. Di seguito una tabella che fornisce una panoramica dello stato attuale dei tempi di rilevamento a livello globale.

METRICA DI RILEVAMENTO	MEDIA DEL 2025	MEDIA DEL 2024	MODIFICA	IMPATTO FINANZIARIO
Tempo medio di identificazione	181 giorni	194 giorni	-13 giorni	2,4 milioni di dollari in media
Tempo medio di contenimento	60 giorni	64 giorni	-4 giorni	1,2 milioni di dollari in media
Ciclo di vita completo della violazione	241 giorni	258 giorni	-17 giorni	4,44 milioni di dollari di media globale
Violazioni entro 200 giorni	~45%	~40%	+5%	3,87 milioni di dollari in media
Violazioni da oltre 200 giorni	~55%	~60%	-5%	$5,01 milioni in media

Traduzione immagine fonte - https://www.totalassure.com/blog/average-time-to-detect-cyber-attack

È importante considerare, altresì, che ogni vettore di attacco presenta sfide differenti per i team di rilevamento. Inoltre, alcuni attacchi richiedono periodi di identificazione significativamente più lunghi.

Ancora, le **compromissioni della catena di approvvigionamento** e le **minacce interne malevole** si classificano costantemente **tra le più difficili da rilevare e contenere**, come si evince dalla tabella sotto riportata.

VETTORE D'ATTACCO	TEMPO PER IDENTIFICARE	TEMPO DI CONTENIMENTO	CRONOLOGIA TOTALE	COSTO MEDIO
Compromissione della catena di approvvigionamento	194 giorni	73 giorni	267 giorni	4,91 milioni di dollari
Insider malintenzionato	200 giorni	60 giorni	260 giorni	4,92 milioni di dollari
Credenziali compromesse	186 giorni	60 giorni	246 giorni	4,31 milioni di dollari
Phishing	175 giorni	65 giorni	240 giorni	4,80 milioni di dollari
Errore interno	153 giorni	60 giorni	213 giorni	3,62 milioni di dollari

Traduzione immagine fonte - https://www.totalassure.com/blog/average-time-to-detect-cyber-attack

2.4 Il paradosso della simulazione: perché gli esercizi non bastano

Le esercitazioni di crisi sono necessarie, ma insufficienti. Il loro design strutturale crea una serie di distorsioni che alterano la percezione della *preparedness*: certezza dello scenario, semplificazione del contesto operativo, progettazione dell'esercizio per il successo piuttosto che per identificare i punti di cedimento.

La risposta non è eliminare le esercitazioni, ma renderle più realistiche attraverso *red team exercise*, *adversarial simulation* e *crisis game* che introducano elementi di sorpresa, degradazione progressiva delle risorse e conflitto di priorità. E, soprattutto, investire in sistemi di risposta e piattaforme di coordinamento che riducano la dipendenza dalla reattività umana nelle fasi più critiche.

2.5 Il ruolo del fattore umano: segnali deboli, cultura, incentivi e disincentivi

Quasi tutti i disastri tecnologici hanno radici profonde in fattori organizzativi e culturali che precedono di anni o decenni l'evento catastrofico. Lo stesso schema si ripete negli incidenti cyber di maggiore impatto.

Prima di ogni incidente grave ci sono quasi sempre indicatori precursori - i.e. anomalie non investigate, *alert* ignorati, *vulnerability assessment* con problemi mai risolti - che la cultura organizzativa non riesce a trasformare in azione preventiva.

E' importante evidenziare che costruire una cultura nella quale segnalare i problemi è premiato - non punito - è una delle leve più potenti per migliorare la resilienza organizzativa e il funzionamento della *War Room*.

3. Il Gap tra compliance e reale capacità di gestione

Molte organizzazioni riscontrano un gap tra la capacità di garantire la compliance ai quadri normativi vigenti e la propria reale capacità di gestione del rischio cyber, a causa di diversi fattori. Vediamo quali.

3.1 La trappola della checklist: quando la conformità diventa fine a sé stessa

La proliferazione normativa degli ultimi anni ha prodotto un effetto al quanto paradossale, ovvero: molte organizzazioni hanno sviluppato sofisticate capacità di gestione della compliance – i.e. team dedicati, strumenti di governance, reporting regolamentare impeccabile - che coesistono con vulnerabilità operative profonde. Un fenomeno che possiamo definire di "*compliance dissonance"* che crea una falsa sicurezza che ritarda gli investimenti in capacità reali.

Inoltre, la trappola della checklist si manifesta quando l'obiettivo dell'organizzazione diventa quello di dimostrare la compliance ai requisiti normativi – i.e. soddisfare i criteri di audit, produrre la documentazione richiesta, ottenere le certificazioni necessarie - piuttosto che sviluppare le capacità operative che quei requisiti intendono promuovere.

La certificazione ISO 27001, il completamento del questionario NIS2 o DORA, l'allineamento con il NIST Cybersecurity Framework diventano badge da esibire, invece di *roadmap* verso la resilienza.

Le cause di questo disallineamento sono molteplici e, precisamente:

- **La misurazione della compliance è più facile della misurazione della capacità reale** - Censire le policy documentate, le formazioni erogate, i controlli implementati è oggettivamente più semplice che valutare se l'organizzazione sia effettivamente in grado di rilevare e di contenere un attacco sofisticato.
- **Il ciclo di audit è periodico e retrospettivo, mentre le minacce evolvono in modo continuo e prospettivo** - Un'organizzazione può essere perfettamente conforme agli standard dell'anno precedente e, al tempo stesso, vulnerabile alle tattiche dell'anno corrente.
- **La compliance è spesso gestita da funzioni separate da quelle operative** – Ad oggi, persiste un dialogo scarso tra chi presidia la conformità normativa e chi gestisce le infrastrutture e le operazioni quotidiane.
- **Gli investimenti in sicurezza tendono a concentrarsi sulle misure verificabili** – Gli investimenti in cybersecurity, spesso, sono rivolti a soluzioni/misure facilmente identificabili dagli auditor, piuttosto che a quelle più efficaci contro le minacce reali.

3.2 Il controllo implementato vs. il controllo efficace

La distinzione tra controllo implementato e controllo efficace è fondamentale e spesso trascurata. Per meglio spiegare: un *firewall* configurato con regole obsolete è un controllo implementato, ma non efficace. Un sistema di rilevamento delle intrusioni che genera 10.000

alert al giorno e il cui team di sicurezza riesce a investigarne il 5% è un controllo implementato, ma non efficace. Un piano di *incident response* mai testato in condizioni realistiche è un controllo implementato, ma non efficace.

Secondo quanto si evince dal recente *"Data Breach Investigations Report" di Verizon*, sistematicamente, la maggioranza degli attacchi che hanno successo sfrutta vulnerabilità note per le quali esistevano già controlli o *patch* disponibili. Pertanto, il problema non è l'assenza di controlli, ma l'incapacità di implementarli in modo consistente, di mantenerli aggiornati di fronte all'evoluzione delle minacce e di integrarli in una logica di sistema.

Inoltre, il gap tra controllo implementato ed efficace è particolarmente evidente in tre aree:

1. **Gestione delle identità e degli accessi (IAM – Identity & Access Management) -** Molte organizzazioni hanno implementato soluzioni MFA e Zero Trust in parte dell'infrastruttura, ma mantengono eccezioni per sistemi legacy, account di servizio con privilegi eccessivi, o integrazioni con terze parti che aprono percorsi di bypass delle protezioni.
2. **Gestione delle vulnerabilità** - I programmi di *patch management* esistono quasi universalmente, ma l'applicazione sistematica delle patch — specialmente su sistemi critici che non possono essere riavviati facilmente — rimane un problema irrisolto per la maggior parte delle organizzazioni.
3. **Backup e recovery** - i backup vengono eseguiti, ma i tempi di ripristino reali in caso di ransomware risultano spesso 3-5 volte superiori alle stime nei piani di *disaster recovery*.

3.3 Verso un modello di maturità integrata: oltre la compliance

La risposta al gap compliance-capacità è adottare la resilienza come stato continuo da mantenere e da migliorare, misurando non solo i controlli implementati ma la loro efficacia, la velocità di risposta agli incidenti, la capacità di ripristino e l'adattabilità alle minacce emergenti.

I framework più avanzati - quali NIST Cybersecurity Framework 2.0 ed ENISA per NIS2 - convergono verso questa visione: la compliance diventa il piano di partenza. **L'obiettivo è un'organizzazione capace di prevenire, rilevare, rispondere e recuperare da incidenti di qualsiasi natura, mantenendo le funzioni critiche operative anche in condizioni avverse**.

4. Il Perimetro esteso: supply chain e rischio delle terze parti

Per decenni la sicurezza informatica è stata pensata come la difesa di un perimetro: una linea di confine materializzata da *firewall* e VPN che separava l'interno sicuro dall'esterno ostile. Tale modello è stato definitivamente superato dalla trasformazione digitale, che ha moltiplicato esponenzialmente i punti di contatto tra l'organizzazione e l'ecosistema esterno.

Oggi un'organizzazione di media dimensione interagisce operativamente con centinaia di fornitori terzi: fornitori SaaS/PaaS/IaaS, provider di IT outsourcing, partner commerciali con accesso ai sistemi, fornitori di infrastruttura critica, prodotti e servizi. Ciascuna di queste

relazioni è un potenziale vettore di rischio: un'intrusione o una negligenza da parte di un fornitore può diventare una porta di accesso all'organizzazione, bypassando completamente le difese perimetrali.

Un programma efficace di *Third Party Risk Management (TPRM)* deve costruire visibilità sistematica attraverso:

- La creazione di un **inventario completo dei fornitori** con classificazione per criticità e tipologia di accesso.
- L'estensione della **valutazione del rischio ai fornitori critici**, attraverso questionari di *security assessment*, richiesta di certificazioni (ISO 27001, SOC 2), o audit diretti.
- Il **monitoraggio continuo del profilo di rischio dei fornitori più critici**, attraverso piattaforme di *Cyber Risk Rati*ng che valutano in tempo reale la postura di sicurezza esterna.
- La definizione di requisiti contrattuali minimi di sicurezza, inclusi diritti di audit, obblighi di notifica degli incidenti e standard di sicurezza minimi.

La governance del TPRM richiede, altresì, la chiarezza su chi è responsabile delle diverse dimensioni del rischio fornitore, ovvero:

- L'ufficio acquisti ha una visibilità sui contratti, ma raramente ha le competenze per valutare il rischio di sicurezza.
- L'IT conosce le integrazioni tecniche, ma non sempre ha visibilità sulla solidità finanziaria del fornitore.
- Il *risk management* ha la metodologia, ma non sempre l'accesso alle informazioni operative.

Pertanto, **un programma efficace richiede una governance cross-funzionale con responsabilità chiare**.

5. NIS2, DORA e il framework europeo della resilienza

Il quadro normativo europeo ha raggiunto una completezza sistemica che merita di essere letta nella sua interezza. NIS2, DORA, Cyber Resilience Act e Direttiva CER costruiscono insieme un ecosistema della resilienza che copre le dimensioni cyber, finanziaria, di prodotto e fisico-organizzativa delle infrastrutture critiche.

L'elemento unificante è l'approccio *risk-based* e *resilience-based*: **le organizzazioni devono dimostrare non solo di aver implementato misure, ma di saper gestire il rischio in modo proporzionato e di poter mantenere o ripristinare rapidamente le proprie funzioni critiche**. La CER completa il quadro estendendo questa logica alla dimensione fisica e organizzativa, chiudendo il cerchio tra cybersicurezza e sicurezza integrata.

Per i risk manager delle organizzazioni soggette a più normative, la sfida è costruire un'architettura di governance della resilienza che risponda a tutti gli obblighi, senza moltiplicare inutilmente i processi.

La soluzione più efficace per una gestione delle crisi realmente funzionale consiste nell'adozione di un **framework di resilienza integrato**, in cui risk assessment, business continuity, sistemi di notifica e metriche di performance siano progettati in modo unitario e coerente per rispondere a tutti i requisiti normativi applicabili.
Tale approccio consente di introdurre declinazioni specifiche per ciascun settore regolamentato, laddove richiesto, superando definitivamente una logica a silos in favore di un **modello olistico di resilienza organizzativa**.

Di fatto, solo attraverso un'integrazione strutturale dei processi e delle responsabilità è possibile rendere l'organizzazione realmente resiliente e dotarla di un modello operativo di *crisis management* capace di funzionare quando la crisi si manifesta nella sua forma reale, ibrida e imprevedibile e non solo negli scenari teorici o di compliance.

6. La War Room: modello operativo per la gestione integrata della crisi

È doveroso ricordare che, quando una crisi colpisce un'organizzazione, la differenza tra una risposta efficace e un disastro gestionale non si misura in tecnologie disponibili o piani documentati: **si misura nella capacità di decidere rapidamente, coordinare competenze diverse, comunicare con chiarezza e mantenere il controllo della narrativa**. È esattamente ciò che la *War Room* è progettata per garantire.

La *War Room*, di fatto, è un modello operativo - non un luogo fisico - che integra competenze tecniche, legali, reputazionali e decisionali sotto un'unica regia. È l'unità di comando e coordinamento che si attiva nel momento della crisi con chiarezza di ruoli, rapidità nelle scelte e allineamento tra tutti gli stakeholder coinvolti.

Il suo obiettivo è ridurre la durata della crisi, limitare gli impatti potenziali e ristabilire rapidamente stabilità e continuità operativa.

6.1 Architettura e componenti della War Room

La *War Room* si articola su quattro dimensioni strutturali interconnesse e, precisamente:

- **Struttura di comando unificata** - Definisce chi è coinvolto nelle decisioni di crisi – i.e. il ***Crisis Management Team*** con ruoli e responsabilità chiare - e come si organizza il coordinamento tra funzioni diverse durante la crisi.
- **Processo strutturato end-to-end** - Definisce il ciclo di vita della gestione della crisi: dall'*early warning* e *detection,* attraverso la valutazione e la dichiarazione della crisi, fino alla risposta, alla *recovery* e alla *review post-incident*.
- **Competenze ibride** – La *War Room* richiede sia le capacità tecniche (i.e. *incident response, forensics, system recovery*) sia quelle non tecniche (i.e. comunicazione di crisi, gestione delle relazioni con i media, interazione con le autorità di vigilanza, supporto psicologico ai team messi sotto stress). Inoltre, un *crisis management* efficace richiede la pre-definizione di un ecosistema di partner esterni – i.e. società di servizi di *incident response*, PR di crisi,

studio legale specializzato e consulenti assicurativi - che garantiscano disponibilità immediata in caso di crisi.

- **Cultura della trasparenza e della decisione** - La *War Room* funziona solo in organizzazioni in cui i problemi vengono segnalati invece che nascosti, i *fail* vengono analizzati, invece che puniti, e la direzione è accessibile e interessata alle questioni di sicurezza. Pertanto, costruire una cultura della resilienza è il punto di partenza su cui tutto il resto si costruisce.

6.2 Dall'*incident response* al *crisis management* multidisciplinare

La distinzione tra *incident response* e *crisis management* non è solo terminologica: **riflette una differenza profonda nella natura delle competenze richieste, nella struttura di governance necessaria e negli stakeholder coinvolti**.

Incident Response	**Crisis Management (War Room)**
Prevalentemente tecnico, gestito dal team di sicurezza con eventuale supporto di specialisti esterni. Si misura in MTTD e MTTR.	Multidisciplinare, coordina leadership aziendale, comunicazione, legal, HR, finance. Si misura in impatto sul business, sulla reputazione e sulle relazioni con gli stakeholder.

Di fatto, un'organizzazione con eccellente *incident response* ma carente in *crisis management* può contenere tecnicamente un attacco, ma subire danni reputazionali e di business considerevolmente superiori all'impatto tecnico dell'incidente. **La *War Room* colma questo gap coordinando entrambe le dimensioni sotto un'unica regia**.

6.3 Piattaforme di coordinamento come infrastruttura operativa

La *War Room* del futuro non si gestisce con fogli Excel e call conference improvvisate. Una categoria di soluzioni tecnologiche sta emergendo con crescente prominenza: **le piattaforme di coordinamento della crisi**, i.e. sistemi *cloud-based* progettati specificamente per supportare la gestione coordinata di incidenti e crisi in organizzazioni complesse e distribuite.

Tali piattaforme integrano:

- **Sistemi di *alerting* e notifica** (i.e. *mass notification*, comunicazioni di emergenza).
- **Gestione delle attività e del flusso di lavoro durante la crisi** (i.e. *task management, ownership, escalation* automatica).
- **Documentazione in tempo reale dell'incidente** (*log* delle decisioni, *audit trail*, evidenze per il reporting normativo).
- **Comunicazione sicura interna ed esterna** (separata dall'infrastruttura ordinaria che potrebbe essere compromessa).
- **Integrazione con sistemi di monitoring e SIEM** per la correlazione degli *alert* tecnici con la risposta operativa.

Il valore di queste piattaforme è soprattutto organizzativo, poiché forniscono una struttura di coordinamento che garantisce una risposta alla crisi più sistematica, più documentabile e più apprendibile.

Inoltre, oggi esistono piattaforme di *crisis management* che fanno uso di AI avanzata, consentendo alle organizzazioni di anticipare, di rispondere e di riprendersi più velocemente, in modo più intelligente e con maggiore sicurezza.

Ancora, i dati di settore evidenziano che le organizzazioni che adottano piattaforme integrate di *crisis management* riportano in media:

34%	**67%**	**< 24h**
Riduzione tempi di risoluzione	**Completezza della documentazione**	**Tempi di notifica normativa**
Incidenti risolti in minor tempo	Miglioramento della qualità del *post-incident reporting*	Rispetto delle scadenze NIS2/DORA per notifica iniziale

6.4 Il modello integrato: sicurezza, continuità, crisi

Il modello operativo più avanzato è quello della convergenza tra le funzioni di sicurezza, *business continuity* e *crisis management* in un'unica architettura di resilienza operativa. In particolare, in questo modello:

- **La funzione di sicurezza** fornisce l'*intelligence* sulle minacce e gestisce la risposta tecnica agli incidenti.
- **La funzione di *business continuity*** garantisce la disponibilità di piani di *recovery* aggiornati e testati per i processi critici.
- **La funzione di *crisis management*** coordina la risposta multidisciplinare quando l'incidente supera i confini tecnici e diventa una crisi organizzativa.

Inoltre, le tre funzioni sono connesse da processi di escalation chiari, metriche condivise, piattaforme tecnologiche che supportano il coordinamento evitando duplicazioni. **Il *risk manager* gioca un ruolo di orchestrazione**: garantisce che la gestione del rischio residuo sia coerente, che le metriche di resilienza siano incorporate nel reporting al board e che il trasferimento del rischio — verso i fornitori e i partner attraverso i contratti, verso i mercati attraverso strumenti innovativi — sia ottimizzato in relazione al profilo di rischio complessivo dell'organizzazione.

7. Da un approccio reattivo a un'architettura integrata di resilienza

Il passaggio da un approccio reattivo a un'architettura integrata di resilienza non è un cambiamento incrementale: è un cambio di paradigma che ridefinisce il modo in cui le organizzazioni pensano al rischio, lo gestiscono e lo governano**. In questa architettura, *crisis management*, coordinamento e trasferimento intelligente del rischio non sono funzioni separate, ma componenti di un unico sistema adattivo**.

DI fatto, i modelli tradizionali di gestione del rischio - costruiti su una logica di compartimentazione, periodicità e trasferimento passivo - sono strutturalmente inadeguati a fronteggiare la realtà di rischi sistemicamente interconnessi, normativamente esigenti e tecnologicamente accelerati, che caratterizzano lo scenario contingente in cui le organizzazioni si trovano ad operare.

Ne consegue che è quanto mai necessario costruire un'architettura integrata della resilienza che non tratti la sicurezza informatica, la continuità operativa e il trasferimento del rischio come silos separati, ma li integri in un sistema adattivo con governance condivisa, metriche comuni e tecnologie connesse.

Pertanto, si consiglia alle organizzazioni di garantire un'architettura che si fonda su cinque pilastri:

1. **Visibilità del rischio reale –** Si tratta di conoscere non solo i rischi teorici, ma la postura di rischio effettiva dell'organizzazione - inclusa la supply chain - attraverso valutazioni continue, non periodiche.
2. **Capacità di risposta strutturata** – È fondamentale investire in *crisis management*, dotandosi di: strutture di governance; processi documentati; competenze ibride; tecnologie di supporto.
3. **Allineamento compliance-capacità** - È necessario superare la logica della compliance come obiettivo finale per adottare quella della **resilienza come stato continuo**, misurando non solo ciò che è stato implementato, ma ciò che è realmente efficace.
4. **Gestione attiva dell'ecosistema** - Si tratta di riconoscere che il perimetro del rischio dell'organizzazione si estende alla rete di fornitori e di partner, e gestirlo con la stessa sistematicità con cui si gestisce quello interno (come anche richiesto dal quadro normativo vigente).
5. **Trasferimento intelligente del rischio** -È importante utilizzare strumenti di risk transfer non come meccanismo di scarico delle responsabilità, ma come componente strategica dell'architettura di resilienza.

7.1 Trasferimento intelligente del rischio come componente sistemica

In un'architettura integrata di resilienza, il trasferimento del rischio non è un add-on finale ma una componente progettata fin dall'inizio. Una strategia integrata si articola su più livelli:

- **Primo livello - *Risk retention* ottimizzata**: definire quanta parte del rischio l'organizzazione è in grado e disposta a trattenere internamente, attraverso riserve di auto-assicurazione, utilizzo di *captive* o definizione di franchigie che riflettano la reale capacità di assorbimento delle perdite.
- **Secondo livello - Trasferimento contrattuale:** redistribuire parte del rischio verso i fornitori attraverso clausole di indennizzazione, requisiti di copertura e limitazioni di responsabilità che riflettano il profilo di rischio della relazione.
- **Terzo livello - Copertura tradizionale:** il trasferimento del rischio residuo attraverso strumenti assicurativi calibrati sul rischio effettivo e non su scenari storici.

- **Quarto livello** - **Accesso ai mercati dei capitali**: per le organizzazioni più strutturate, *cat bond, insurance-linked securities* e soluzioni parametriche che permettono di coprire scenari catastrofali non disponibili attraverso strumenti tradizionali.

In questo modello le metriche di resilienza operativa – i.e. MTTD, MTTR, RTO, RPO effettivi - diventano fattori di pricing e di negoziazione, creando incentivi finanziari diretti per migliorare la capacità di risposta.
Inoltre, le organizzazioni che possono dimostrare una capacità di documentazione strutturata - abilitata dalla *War Room* e dalle sue piattaforme - ottengono condizioni migliori e processi di liquidazione più rapidi.

7.2 Il modello operativo del futuro

Il modello operativo che emerge è quello di una convergenza tra sicurezza informatica, *business continuity management* e trasferimento del rischio, con la *War Room* come sistema nervoso centrale. In termini pratici:

- La **valutazione del rischio residuo** dopo i controlli di sicurezza diventa l'input diretto per le decisioni di trasferimento, eliminando il disallineamento tra ciò che viene dichiarato e ciò che è effettivamente implementato.
- I **piani di *business continuity*** incorporano esplicitamente le procedure di documentazione del sinistro e le procedure di notifica normativa, riducendo i tempi di attivazione in caso di crisi.
- Le **piattaforme di coordinamento** connettono la risposta tecnica agli incidenti con la gestione della crisi organizzativa, documentando automaticamente le evidenze necessarie per il reporting normativo e per la gestione del rischio.
- Le **metriche di resilienza operativa** diventano fattori di *governance del board*, sostituendo progressivamente il solo *reporting di compliance*.

Il *risk manager* in questo modello non è più un compratore di protezione, ma un orchestratore della resilienza che gestisce il profilo di rischio residuo, coordina le strategie di *retention* e trasferimento, oltre ad usare la relazione con i partner esterni come leva per accedere a competenze, dati e servizi che migliorano la capacità di resilienza dell'organizzazione.

Conclusione: verso un'architettura integrata della resilienza

I modelli tradizionali di gestione del rischio, costruiti su una logica di compartimentazione, periodicità e trasferimento passivo, sono strutturalmente inadeguati a fronteggiare la realtà di rischi sistemicamente interconnessi, normativamente esigenti e tecnologicamente accelerati che caratterizzano lo scenario contingente.

La risposta non è un aggiustamento marginale di strumenti e processi esistenti. È un cambio di paradigma che richiede di costruire **un'architettura integrata della resilienza, al centro della**

quale si trova la *War Room* come modello operativo permanente e non come misura emergenziale.
Pertanto, le organizzazioni che affronteranno con successo le crisi dei prossimi anni non saranno quelle che avranno costruito in anticipo un sistema adattivo in cui *crisis management*, coordinamento e trasferimento intelligente del rischio operano come un'unica architettura integrata, sempre pronta, sempre aggiornata, sempre testata. Questo è il vero vantaggio competitivo della resilienza.

Inoltre, il contesto normativo europeo - con NIS2, DORA, il Cyber Resilience Act e la Direttiva CER - fornisce le leve regolatorie e gli incentivi necessari per accelerare questa trasformazione. DI fatto, i *framework risk-based* e *resilience-based* creano un allineamento tra gli obiettivi dei regolatori e le necessità operative delle organizzazioni.

Per le organizzazioni nel loro complesso, ciò richiede di riconoscere che la resilienza non è un costo da minimizzare, bensì un investimento strategico da ottimizzare.

Concludendo, le organizzazioni che costruiranno questa capacità nei prossimi anni saranno quelle capaci di sopravvivere alle crisi che inevitabilmente arriveranno, dimostrando la propria robustezza rispetto ai competitor che non l'hanno fatto.

Key takeaways:

Appendice: riferimenti normativi e framework di riferimento

Normative europee

- Direttiva NIS2 (UE 2022/2555) — Sicurezza delle reti e dei sistemi informativi, recepimento ottobre 2024
- Direttiva CER (UE 2022/2557) — Resilienza dei soggetti critici, recepimento ottobre 2024
- Regolamento DORA (UE 2022/2554) — Resilienza operativa digitale del settore finanziario, applicazione dal 17 gennaio 2025
- Cyber Resilience Act (UE 2024/2847) — Requisiti di cybersicurezza per i prodotti con elementi digitali
-

Framework e standard internazionali

- NIST Cybersecurity Framework 2.0 (2024) — Framework per la gestione del rischio cyber
- ISO/IEC 27001:2022 — Sistema di gestione della sicurezza delle informazioni
- ISO 22301:2019 — Business Continuity Management System
- ENISA Guidelines NIS2 — Linee guida dell'Agenzia UE per la Cybersicurezza

Altri materiali e Studi

- ENISA Threat Landscape 2025 — Panorama delle minacce informatiche in Europa
- Verizon Data Breach Investigations Report 2025
- IBM — Cost of a Data Breach Report 2025

Whitepaper a cura di **Federica Maria Rita Livelli**

Consulente in Risk Management & Business Continuity, svolge un'attività di diffusione e sviluppo della cultura della resilienza presso varie istituzioni e università italiane e straniere. È membro de: CLUSIT – Direttivo; BCI - Cyber Resilience Group; FERMA Digital Committee. Svolge attività di docente di moduli di resilienza presso l'Università Genova – Master Infrastrutture Critiche, l'Università di Udine -Master di Intelligence & ICT e l'Università di Verona – RiskMaster.
Relatrice e moderatrice in diversi seminari, conferenze nazionali ed internazionali, autrice di numerosi articoli e white paper su diverse riviste italiane e straniere.
Co-autrice de: Rapporto Clusit - Cyber Security (ed. dal 2020 ad oggi); Libri tematici CLUSIT rif. Intelligenza Artificiale (2020) e Rischio Cyber (2021), Supply Chain Risk (2023); "Lo Stato in Crisi" ed. Angeli (2022); "The ACP book of best practices 3rd edition - Important topics within resilience (2025).
