Le capacità di resilienza delle aziende italiane. Indagine di SPIKE REPLY ed EVERBRIDGE con AIPSA

di Federica Maria Rita Livelli - Business Continuity & Risk Management Consultant (*)

Scenario

Lo scenario erratico in cui stiamo vivendo mette a dura prova la resilienza delle nostre organizzazioni.
Spike Reply ed **Everbridge** - in collaborazione con **AIPSA** - hanno recentemente svolto un'indagine per valutare il livello di capacità delle aziende italiane nel gestire i rischi, la continuità organizzativa ed operativa e identificare le strategie atte a garantirne la resilienza.
L'indagine - presentata da Spike Reply ed Everbridge lo scorso 24 marzo durante l'evento patrocinato da AIPSA e titolato *"La capacità di resilienza delle aziende italiane: scenari attuali e prospettive future"* – ha coinvolto 45 medio-grandi organizzazioni operanti sia sul territorio nazionale sia a livello internazionale.

Il livello di capacità delle organizzazioni nel gestire eventi critici e nel garantire la continuità del business è stato misurato utilizzando un Maturity Model - strutturato in cinque livelli (i.e. in ordine crescente: ad hoc, reattivo, gestito, proattivo, ottimizzato) e riferito a quattro fasi di gestione degli eventi critici, quali:

- valutazione di minacce e impatti;
- localizzazione
- risposta alla manifestazione dell'evento
- analisi della capacità di prendere decisioni data-driven prima (i.e.: identificazione dei rischi prima che si trasformino in eventi critici), durante e dopo l'evento critico/dirompente

I risultati dell'indagine hanno evidenziato come la maggior parte delle organizzazioni coinvolte - pur avendo predisposto procedure per la gestione degli eventi critici - non effettui regolari aggiornamenti dei modelli, rischiando di prepararsi inadeguatamente alla gestione di un evento critico.
Inoltre, risulta quanto mai importante individuare e censire correttamente i cosiddetti asset critici che, nella maggior parte dei casi, sono gestiti in modo integrato, pur risultando ancora diffusi i sistemi basati su fogli di calcolo o piattaforme interne (soprattutto per gli asset materiali). Ne consegue che risulta difficile garantire sia una visione globale degli assetti, sia la raccolta di informazioni coerenti.
Le organizzazioni, per quanto riguarda le risorse umane, utilizzano sia piattaforme di localizzazione automatizzate per censire/mappare il personale viaggiante o gli expatriate sia piattaforme centralizzate di HR Management per i dipendenti in sede.

Di seguito i risultati dell'analisi del Livello di Maturity delle organizzazioni intervistate:

- **Livello di Maturity "Reattivo" nella fase di "valutazione" - Il 43%** identifica i rischi prima che si trasformino in eventi critici, ma non sufficientemente in anticipo da garantire ottimali tempi di risposta e di recupero. I rischi sono individuati solitamente tramite indagini via internet; mentre le valutazioni in termini di gravità e di impatto sugli asset sono eseguite manualmente, rallentando così l'attivazione dei piani di risposta e compromettendo il controllo della situazione in caso di evento dirompente.

• **Livello di Maturity "Gestito" nella fase di "localizzazione" - Il 38%** localizza e comunica efficacemente con i team di risposta e con chi è stato impattato dall'evento dirompente, i dipendenti e gli stakeholder, utilizzando sistemi di geolocalizzazione o check-in ed Emergency Call System. Tuttavia, solo il 5% delle organizzazioni ha un sistema unificato per la gestione di crisi o eventi critici.
• **Livello di Maturity "Gestito" nella fase di risposta alla manifestazione dell'evento - Il 46%** riesce a mitigare l'impatto di un evento dirompente e a comunicare efficientemente con le risorse impattate. Tuttavia, il 48% delle organizzazioni non risultano avere in essere una procedura di escalation sufficientemente automatizzata atta a ottimizzare i flussi informativi, ridurre tempi di reazione, garantire una migliore risposta all'emergenza.
• **Livello di Maturity "Gestito" nell'analisi della capacità di prendere decisioni data-driven prima, durante e dopo l'evento critico/dirompente - il 43%** effettua la raccolta ed il monitoraggio dei dati in tempo reale, impiegando processi standardizzati che, pur richiedendo spesso un intervento manuale, permettono di: riesaminare regolarmente le informazioni; anticipare eventi futuri; apportare migliorie ai piani di risposta. Inoltre, risulta che l'aggregazione dei dati richiede spesso un intervento manuale.

Nessuna delle organizzazioni ha raggiunto il Livello "Ottimizzato" mentre, in termini di "Livello Medio di Maturity", la situazione è la seguente:
• **"Gestito" - Il 43,20%** dimostra buone capacità di risposta agli eventi critici, grazie ad un approccio maturo durante le fasi di identificazione e valutazione delle minacce, di individuazione dei team di risposta, di predisposizione delle strategie e dei piani di gestione delle crisi (che vengono testati ed aggiornati regolarmente).
• **"Reattivo" - Il 35,10%** dispone di piani e di protocolli di risposta che vengono attivati solo al verificarsi dell'evento dirompente.
• **"Proattivo" - Il 16.20%** ha processi solidi e tecnologie per l'identificazione anticipata dei rischi. Inoltre, gestisce in modo controllato l'evento critico, potendo contare anche sulla collaborazione degli stakeholder.

Conclusioni e prospettive future
Il quadro scaturito dall'indagine non fa che confermare come i principi di Risk Management, Business Continuity e Cybersecurity possono convertirsi in leve strategiche in grado di gestire e garantire la resilienza operativa e organizzativa in scenari sempre più erratici e digitalizzati.
Ovvero, le organizzazioni - di fronte alla cosiddetta "imprevedibile certezza del rischio" - devono dimostrare di essere più agili, flessibili e adattive, acquisendo il massimo grado di conoscenza e consapevolezza sia di sé (come organizzazione e come persone) sia del contesto interno ed esterno in cui si opera, oltre a garantire l'implementazione di sistemi di gestione efficaci ed efficienti in continuo aggiornamento e miglioramento.
Di fatto, si tratta di concepire l'organizzazione resiliente come un'orchestra i cui "esecutori" conoscono il proprio repertorio e contribuiscono insieme all'esecuzione ottimale della "sinfonia organizzativa". Ne consegue che, in una trasposizione "ardita", Risk Management & Business Continuity, Cybersecurity e Security Manager, unitamente alle altre funzioni di sicurezza, dovranno "suonare all'unisono" e favorire organizzazioni che operano in modo fluido e senza silos.

Federica Maria Rita Livelli
In possesso di certificazione Business Continuity - AMBCI BCI, UK e CBCP DRI, USA, Risk Management FERMA Rimap®, consulente di Business Continuity & Risk Management, svolge attività di diffusione e di sviluppo della cultura della resilienza presso varie istituzioni ed università.
Socia AIPSA (Italian Association of Security Managers) ed UNI (Italian Regulatory Institute); Board member di: ANRA, BCI Italy Chapter, CLUSIT Scientific Committee e Commissioni tecniche UNI.
Docente di moduli ISO 22301 e 31000 presso diverse università (POLIMI–BOCCONI, Verona, Cagliari, Padova, Statale di Milano e LIUC Castellanza).
Relatrice e moderatrice in seminari, conferenze nazionali ed internazionali.
Autrice di articoli su numerose riviste online, Ha partecipato, in qualità di coautrice, a: Edizioni 2020, 2021 e 2022 del Rapporto Clusit - Cyber Security; Libri tematici CLUSIT rif. Intelligenza Artificiale (2020) e Rischio Cyber (2021); Libro "Lo Stato in Crisi" ed. Angeli.