Anticipare e non subire le crisi

L'evento Motivation Night, tenutosi il 27 marzo presso il LAC di Lugano, promosso dal PRL Lugano e dedicato al tema "Le nuove sfide per le aziende tra geopolitica e guerre ibride" è stato un'occasione per riflettere sull'impatto che le attuali crisi internazionali hanno sull'attività delle imprese. Ce ne parlano Luca Tenzi, esperto di sicurezza internazionale, e Alessandro Trivilini, esperto di sicurezza informatica.

Luca Tenzi

Alessandro Trivilini

Perché la geopolitica è diventata una questione concreta anche per le aziende?

Luca Tenzi: «La geopolitica, un framework che ho avuto modo di testare sul campo in America Latina, lavorando per Telecom Italia all'inizio degli anni 2000, ovvero la sostituzione della logica del conflitto militare con quella del confronto economico-commerciale tra Stati, non è una novità nei piani strategici delle grandi aziende. La globalizzazione ha semplicemente portato in superficie ciò che era sempre stato soggiacente. Le PMI, storicamente meno esposte a questo confronto, ne hanno preso coscienza solo quando hanno iniziato a guardare oltre i confini nazionali, spinte dalla necessità di crescere in mercati nuovi e più lontani.
Il salto di qualità è arrivato con le crisi sistemiche. Patrick Trancu, crisis manager luganese e tra i massimi esperti europei della materia, ne identifica cinque nei primi vent'anni di questo secolo: l'11 settembre 2001, la crisi finanziaria del 2008, la pandemia, la guerra in Ucraina e i recenti conflitti in Medio Oriente. A quel punto, ignorare la geopolitica, o il rischio geopolitico, non era più un'opzione. Per le aziende, grandi e piccole, questo ha significato una cosa concreta: l'analisi del rischio geopolitico ha smesso di essere una variabile di contesto ed è diventata un driver strategico. Il foresight, la capacità di leggere ciò che sta per accadere prima che accada, è diventato una competenza organizzativa, non un esercizio riservato ai think tank».

Qual è l'errore più frequente che compiono le aziende quando sottovalutano il rischio geopolitico?

Luca Tenzi: «L'errore più frequente che osservo è la sistematica sottovalutazione dell'impatto indiretto degli eventi geopolitici. Le aziende, specie le PMI, tendono a valutare il rischio in modo lineare: guardano all'evento in sé, raramente alle sue onde d'urto. Le grandi aziende, proprio per la loro presenza più capillare, dispongono di più sensori che consentono una lettura più tempestiva di eventi "locali" con portata regionale o globale. È esattamente qui che entra in gioco l'effetto farfalla, quel principio della teoria del caos secondo cui piccole variazioni nelle condizioni iniziali producono effetti amplificati e imprevedibili su sistemi complessi. L'interdipendenza creata dalla globalizzazione ha reso le supply chain delle PMI straordinariamente vulnerabili a questa dinamica. Il cambio di governo in un paese africano può sembrare distante, ma può ridisegnare relazioni commerciali decennali, spostare l'accesso a materie prime critiche, o favorire un competitor che operava fino a ieri in posizione marginale. E non serve guardare così lontano: per il Ticino, i cambiamenti di priorità politiche dell'attuale governo italiano hanno impatti economici e di relazioni di vicinato tutt'altro che trascurabili. Qui entrano in gioco due concetti che ritengo fondamentali. Il primo, forse il più conosciuto, è il Black Swan di Nassim Taleb, l'evento ritenuto improbabile che, quando accade, ha un impatto devastante che i modelli di rischio tradizionali semplicemente non contemplavano. L'esempio più eloquente resta la pandemia. Il secondo è il Gray Rhino di Michele Wucker, forse meno noto alle nostre latitudini ma altrettanto insidioso: il rischio ovvio, visibile, ad alta probabilità, che le organizzazioni scelgono, consapevolmente o no, di ignorare. La tensione USA-Cina sulle tecnologie, la fragilità energetica europea, la dipendenza dalle terre rare: erano tutti gray rhinos ben prima di diventare emergenze. L'errore, in sintesi, non è sempre non aver visto il rischio. Spesso è averlo osservato, non analizzato e di conseguenza non aver agito».

Quando un'azienda può dire di essere davvero resiliente?

Luca Tenzi: «Un'azienda davvero resiliente non ambisce a tornare al punto di partenza. Ambisce a uscire dalla crisi in una posizione diversa, e possibilmente più forte più competitiva. La vera resilienza è una capacità sistemica, nella gestione della complessità, che si costruisce prima che la crisi arrivi, ad esempio attraverso la diversificazione delle supply chain, una cultura del rischio diffusa a tutti i livelli dell'organizzazione, e una pratica strutturata di scenario planning.
Per rendere il concetto concreto, mi piace usare una metafora. Immaginiamo un'azienda resiliente come un veliero a tre alberi: a seconda della forza delle onde, delle correnti e dei venti, il comandante userà più o meno velatura, ridurrà i bordi di navigazione, cambierà rotta. Non si ferma, adatta, i tempi di percorrenza non saranno quelli previsti ma l'obiettivo rimane lo stesso. Ecco cosa dovrebbe fare la leadership di una PMI, considerarsi il comandante di quel veliero, con la capacità di leggere il mare prima che la tempesta sia sopra di lui».

Se dovesse lanciare un messaggio agli imprenditori presenti all'evento "Motivation Night" quale sarebbe?

Luca Tenzi: «Credo che il messaggio che abbiamo potuto condividere du-

rante la serata sia che il rischio geopolitico è diventato un rischio d'impresa anche per le PMI ticinesi.
Non è più una variabile di contesto, è una variabile strategica che appartiene all'agenda di ogni imprenditore, indipendentemente dalla dimensione aziendale. In Svizzera le PMI rappresentano circa. il 95% del tessuto imprenditoriale e generano due terzi dei posti di lavoro del paese.
Non sono la parte secondaria del sistema, sono il sistema. E le aziende ticinesi, per la loro posizione e per le relazioni che intrattengono con l'Italia e con il mercato europeo, si trovano in prima fila in questa nuova dinamica, non solo per scelta, ma per vocazione territoriale.
Quello che manca, nella maggior parte delle PMI che ho potuto incontrare, non è la capacità di reagire, abbiamo aziende con una storia decennale che hanno dimostrato di saper navigare in "mari mossi", è l'abitudine di anticipare. Di leggere i segnali deboli prima che diventino crisi. Di distinguere un gray rhino, un rischio visibile e ignorato, da un problema che poteva essere gestito con anticipo».

Quanto è già presente, oggi, il fronte digitale nella vita quotidiana delle aziende?
Alessandro Trivilini: «Per rispondere correttamente bisogna distinguere tra informatizzazione e digitalizzazione. Molte aziende oggi sono informatizzate: utilizzano software, strumenti digitali e piattaforme per lavorare meglio. Ma essere digitali è un'altra cosa. La vera digitalizzazione implica ripensare i processi, automatizzarli e renderli più efficienti grazie alla tecnologia. Su questo fronte, molte aziende sono ancora indietro. Nonostante i progressi e l'accelerazione portata dall'intelligenza artificiale, siamo ancora all'inizio del percorso: il digitale è presente, ma il suo potenziale è solo in parte sfruttato.

Qual è oggi la vulnerabilità più sottovalutata dalle aziende?
Alessandro Trivilini: «La vulnerabilità più sottovalutata oggi è la formazione del personale. Molte aziende investono in tecnologie avanzate, ma trascurano l'aggiornamento delle competenze delle persone. Questo è un problema crescente, soprattutto perché i criminali informatici stanno utilizzando l'intelligenza artificiale per rendere gli attacchi sempre più credibili e mirati. Oggi un'email di phishing può essere scritta in modo perfetto o simulare comunicazioni reali, rendendo molto più difficile riconoscere il pericolo. Senza una formazione continua, anche i migliori sistemi di sicurezza possono essere aggirati.

Ci sono segnali che un'azienda tende a ignorare e che invece dovrebbero allarmarla?
Alessandro Trivilini: «Oggi, uno dei segnali più allarmanti che un'azienda tende a ignorare è l'evoluzione delle normative in materia di sicurezza, come DORA e NIS2, che richiedono un approccio collaborativo alla gestione della cybersecurity. Queste normative sottolineano l'importanza di coinvolgere non solo i dipendenti interni, ma anche clienti, fornitori e consulenti nella sicurezza delle informazioni. Le aziende devono adottare strategie che includano una valutazione del rischio residuo, tenendo conto delle interazioni con tutti gli attori coinvolti nella catena del valore. È fondamentale che le aziende sviluppino una cultura della sicurezza che promuova la consapevolezza e la responsabilità collettiva».

Se un'azienda volesse fare un primo vero passo per alzare il proprio livello di sicurezza, da dove dovrebbe cominciare?
Alessandro Trivilini: «Il primo passo concreto è dotarsi di un piano di risposta agli incidenti. Non basta prevenire: bisogna essere pronti a reagire. Ogni azienda dovrebbe sapere in anticipo cosa fare in caso di attacco, chi è responsabile e quali azioni intraprendere nelle prime ore, che sono le più critiche. A questo va affiancata una governance della sicurezza chiara e su misura, che definisca ruoli, responsabilità e processi. La sicurezza efficace non è solo tecnologia, ma organizzazione, preparazione e capacità di risposta».

Da sinistra: **Paolo Morel**, **Luca Tenzi**, **Laura Zucchetti** e **Alessandro Trivilini**