PREMIO GIUSEPPE TALIERCIO

3° EDIZIONE – ANNO 2023

Abstract tesi vincitrice

fondirigenti

UNIVERSITÀ BOCCONI E POLITECNICO MILANO

GRADUATE SCHOOL

Corso di Laurea Magistrale in Cyber Risk Strategy and Governance

Tesi di Laurea Magistrale

Leadership Competences in Cyber Risk Management. Extending Current Research Perspectives

Relatore: **CANDIDATA**

Prof. Gianluca Salviotti **Dott.ssa Chiara D'Ignazio**

A.A. ACCADEMICO 2022-2023

Abstract

La rapida e diffusa digitalizzazione sta rivoluzionando tutte le attività e i processi sociali che caratterizzano i nostri Paesi, rendendoli sempre più intelligenti ed efficienti. Questa trasformazione offre opportunità senza precedenti, ma introduce anche nuovi rischi, ampliando la superficie di attacco dei sistemi fisico-cibernetici sempre più interconnessi. Nel mondo attuale, sempre più connesso digitalmente, le minacce e gli incidenti informatici rappresentano un rischio crescente per le attività sociali. La criminalità informatica, in particolare gli attacchi ransomware, stanno diventando sempre più frequenti, sofisticati e diffusi, colpendo governi, individui e aziende private in tutto il mondo.
Gli incidenti informatici particolarmente rilevanti possono avere costi e danni ingenti, che hanno il potenziale di portare al fallimento delle aziende e a gravi impatti sull'economia, sulle infrastrutture critiche e sulla sicurezza nazionale. Pertanto, le crisi organizzative legate alla sicurezza informatica sono percepite come uno dei pericoli più urgenti del nostro tempo. In questo contesto critico, è ampiamente riconosciuto che la gestione delle crisi informatiche può avere un impatto significativo sul successo e sulla sostenibilità a lungo termine delle aziende. Proprio per questo, è fondamentale comprendere quali capacità, processi e strumenti siano efficaci per affrontare queste crisi. La letteratura attualmente esistete e consolidata sulla gestione delle crisi identifica competenze di leadership che possono essere utilizzate per mitigare gli impatti di una crisi di tipo tradizionale. Tuttavia, le ricerche sull'efficacia di queste competenze nella gestione delle nuove e più attuali crisi informatiche sono ancora in corso. Questa tesi si propone di ampliare le attuali conoscenze in questo campo di ricerca senza dubbio fondamentale, analizzando il caso di Maersk, un'azienda di logistica globale che nel 2017 è stata vittima di uno dei più devastanti attacchi ransomware. La tesi utilizza un modello di leadership nato per gestire le crisi tradizionali come lente di analisi.

Coerenza della tesi con i temi indicati nel bando del Premio Taliercio:

Il Premio Giuseppe Taliercio è stato istituito con l'obiettivo di promuovere nelle giovani generazioni il ricordo della figura e dei valori del manager a cui la Fondazione è intitolata, e per approfondire l'impegno della stessa Fondazione nella ricerca sulle grandi trasformazioni che interesseranno il contesto economico-produttivo e della resilienza delle imprese.

Oggi la resilienza delle imprese non può prescindere dal concetto di cyber-security e cyber-resilience, due temi che a livello manageriale sono diventati importantissimi anche a seguito delle nuove regole e requisiti del SEC a cui sono soggette da quest'anno le aziende americane quotate. In un contesto dinamico, ricco di minacce informatiche sempre più all'avanguardia e difficili da contrastare, per un manager risulta fondamentale acquisire le skills e le competenze necessarie per integrare la cybersecurity nella strategia aziendale e per implementarla a livello di competenze, tecnologie e processi, in modo da garantire la sicurezza e la sostenibilità della propria azienda. È necessario inoltre essere pronti ad affrontare una cyber-crisi, qualora un attacco dovesse andare a buon fine. A questo scopo la mia tesi ha l'obiettivo di individuare le competenze e le skills, hard e soft, che i manager devono adottare per affrontare con successo una crisi informatica con minimo impatto sulla propria realtà aziendale. Dunque, tra le varie tematiche inerenti al premio di laurea, la mia tesi rientra nella prima, ovvero: *Innovazione (trasformazione digitale dei processi aziendali produttivi, logistici, di vendita; governo dei dati; cybersecurity)*.

Obiettivi della tesi:

Negli ultimi anni, le ricerche si sono concentrate sull'indagine dei fattori che si dimostrano influenti nell'affrontare una crisi organizzativa tradizionale. Tra questi, la reattività della direzione, le competenze di leadership, i team coordinati e i dipendenti motivati e resilienti sono stati riconosciuti come i principali determinanti del guadagno o della perdita di valore dell'azienda nel lungo termine (Bundy et al., 2017; James et al., 2011; Pwc e Oxford-Metrica, 2020; Wart e Kapucu, 2011; Williams et al., 2017; Wooten e James, 2008).

Data la crescente frequenza e gravità dei cybercrimini su scala globale, è ragionevole suggerire che l'identificazione di fattori specifici che aiutano le aziende ad affrontare le crisi legate al cybercrimine (di seguito denominate crisi cibernetiche) offrirebbe ulteriori preziosi spunti di riflessione sia ai ricercatori che ai professionisti. Tuttavia, sebbene le crisi cibernetiche siano ampiamente riconosciute come una delle minacce più gravi per la nostra società, la letteratura accademica attualmente presenta pochissime ricerche su questo argomento. Esiste ancora un vuoto di ricerca critico su come le aziende possano sviluppare processi e capacità ottimali di gestione delle crisi cibernetiche, in particolare in relazione alle competenze di leadership (Salviotti et al., 2023).

Uno dei primi lavori che affronta questo specifico gap è "Understating the Role of Leadership Competencies in Cyber Crisis Management: A Case Study" (Salviotti et al., 2023) originariamente presentato nei Proceedings of the 56th Hawaii International Conference on System Science 2023 (di seguito denominato documento di riferimento), che si concentra specificamente sul determinare se le competenze di leadership identificate dalla letteratura come efficaci per la gestione delle crisi tradizionali siano effettivamente valide anche nei contesti di crisi cibernetica. Come sottolineano gli autori, "In vista della rapida evoluzione dei cybercrimini e delle loro conseguenze negative per le organizzazioni e la società, esiste l'esigenza cruciale di contribuire ad aumentare la conoscenza delle crisi legate al cybercrimine. Di conseguenza, l'argomento investigato è sia attuale che urgente". Questa tesi è concepita come un'estensione del documento di riferimento con l'obiettivo di contribuire ad aumentare la conoscenza in questo campo essenziale.
I risultati del documento di riferimento hanno iniziato a fare luce su quali capacità siano efficaci per affrontare le crisi cibernetiche. In particolare, sebbene sia stato riscontrato un buon livello di allineamento tra gli scenari tradizionali e i contesti di crisi cibernetica, le competenze di leadership necessarie per gestire le crisi cibernetiche non sono necessariamente uguali a quelle che la letteratura accademica suggerisce per gestire con successo le crisi tradizionali. I risultati e la discussione degli autori hanno iniziato a fare luce sull'argomento, ma è necessario un ulteriore approfondimento per fornire preziosi spunti di riflessione, modelli e quadri di riferimento nel campo della gestione delle crisi cibernetiche. Attraverso l'analisi di diversi dati, questa tesi mira esattamente a rispondere a tale esigenza. In particolare, utilizza lo stesso approccio per indagare un diverso case study, che presenta diverse caratteristiche in termini di tipo di azienda, modello di business e geografia: il collasso globale della supply chain di Maersk. I risultati dell'analisi eseguita offrono la possibilità di confermare o smentire i risultati del documento di riferimento, nonché il potenziale di rivelare nuovi elementi che non sono stati considerati. Questo, insieme ai risultati del documento di riferimento, può essere utilizzato come una preziosa fonte di dati per costruire un quadro di riferimento per le competenze di leadership in caso di crisi cibernetica.

Attività di ricerca svolte per l'elaborazione: (es. sperimentazioni, questionari, interviste, utilizzo di strumenti digitali, applicativi, analisi desk o ricerche field, ecc.)

Per costruire la narrazione e procedere con l'analisi del caso Maersk, sono state utilizzate molteplici fonti di dati, tra cui interviste, podcast, documenti e articoli. Il caso scelto presenta infatti una grande quantità di informazioni pubbliche e testimonianze rilasciate dai top manager direttamente coinvolti in tutte le attività svolte durante il cyber attacco. Molti di loro hanno partecipato a panel discussion, interviste e podcast in cui hanno avuto la possibilità di descrivere l'attacco dalla loro prospettiva e condividere la loro opinione personale su ciò che è accaduto. Queste testimonianze hanno rappresentato dati molto preziosi, che sono stati utilizzati come fonte primaria per ricostruire la narrazione. Per completare la narrazione e fornire maggiori dettagli sullo sviluppo degli eventi, sono state utilizzate anche diverse fonti secondarie di valore, tra cui pagine web ufficiali, case study e articoli. Infine, sono stati analizzati anche i rapporti annuali di Maersk dal 2016 al 2021 e l'account Twitter ufficiale dell'azienda, in quanto utili per comprendere eventuali cambiamenti nel piano strategico, organizzativo e finanziario dell'azienda in risposta all'attacco. La costruzione di significato dai dati raccolti è stata il risultato di una procedura di analisi progressiva che, attraverso l'adozione di diversi passaggi induttivi, ha permesso di passare dai dati allo sviluppo della teoria. Sebbene non esista una procedura standardizzata per condurre l'analisi dei dati qualitativi, vari ricercatori hanno pubblicato linee guida e processi per l'analisi delle narrazioni. Tra questi, la procedura scelta e utilizzata in questa tesi è la stessa adottata dagli autori del documento di riferimento, ovvero l'analisi tematica narrativa.

L'analisi tematica narrativa si compone di cinque fasi:

1. Organizzazione e preparazione dei dati raccolti
2. Ottenere un senso generale delle informazioni
3. Eseguire il processo di codifica
4. Categorizzare in temi
5. Interpretazione dei dati

Conclusioni determinate dai risultati ottenuti dai punti di cui sopra:

Confrontando e integrando i risultati ottenuti dall'indagine delle due maggiori crisi informatiche vissute da Maersk e Norsk Hydro, questa tesi offre preziose implicazioni manageriali che possono guidare i leader nel rafforzare la postura di sicurezza informatica della propria azienda e nell'acquisire gli strumenti, le competenze e le abilità necessarie per navigare efficacemente attraverso una crisi informatica.

Nel complesso, la tesi evidenzia la necessità di una postura di sicurezza informatica completa e proattiva che integri gli aspetti di protezione, reazione e ripristino. Infatti, il panorama delle minacce in continua evoluzione e sempre più complesso rende impossibile per le aziende azzerare completamente il rischio di essere colpite da un attacco informatico. Pertanto, è fondamentale allocare investimenti e risorse non solo per proteggere l'organizzazione, ma anche per rafforzare la sua capacità di risposta nel caso in cui si verifichi una crisi informatica.

Lo sviluppo di una strategia di sicurezza informatica allineata con le strategie aziendali e digitali, nonché l'identificazione delle funzioni chiave, delle vulnerabilità e degli attori delle minacce, è essenziale per un'azienda per prioritizzare le azioni e allocare le risorse in modo efficace. Ciò richiede ai top manager di iniziare a percepire la sicurezza informatica come un abilitatore del business piuttosto che come un costo da minimizzare.

Gli investimenti in sicurezza informatica dovrebbero seguire un approccio basato sul rischio che richiede ai leader di ottenere piena visibilità sia del contesto interno che esterno in cui opera l'azienda. Ciò consentirà loro di definire politiche e linee guida di sicurezza specificamente adattate alle esigenze dell'azienda. Una volta definite, tali procedure devono essere integrate nelle operazioni della realtà aziendale in modo che tutti i suoi dipendenti, indipendentemente dal loro profilo e dalle loro posizioni, le seguano nelle loro attività quotidiane.

Inoltre, è anche fondamentale pianificare e prepararsi a una possibile crisi. È importante definire un piano di continuità aziendale e ripristino che deve essere continuamente esercitato e mantenuto. Devono essere sviluppati programmi di formazione, sensibilizzazione ed educazione per fornire ai dipendenti le competenze e le abilità necessarie per rispondere a un attacco informatico. Le attività di formazione dovrebbero inoltre mirare allo sviluppo di competenze trasversali e soft (lavoro di squadra, creatività e capacità decisionale in condizioni di rischio e pressione temporale) che possono essere il fattore differenziante durante una crisi.

Anche la cultura e i valori aziendali dovrebbero ricevere particolare attenzione da parte dei top manager, poiché svolgono un ruolo fondamentale nel promuovere la collaborazione tra gli attori, l'impegno dei dipendenti e la condivisione delle informazioni, che sono elementi essenziali per aumentare la postura di sicurezza dell'azienda.

Durante una crisi, la comunicazione trasparente e aperta, la leadership presente e reattiva e le relazioni con il network esterno sono fattori critici per garantire una risposta efficace. Il coinvolgimento dei leader in tutte le attività legate alla crisi e la creazione di una rete con stakeholder esterni sono essenziali per mantenere l'agilità e la reattività dell'azienda durante la crisi e per aumentare la postura di sicurezza informatica e la resilienza dell'intera catena del valore in cui essa si inserisce.

Sulla base di questa analisi e raccomandazioni, il lavoro futuro potrebbe concentrarsi sull'ulteriore affinamento dei concetti trattati in modo più strutturato con l'obiettivo finale di sviluppare un modello di riferimento che possa guidare i top manager delle aziende nella costruzione delle competenze e delle abilità necessarie per affrontare in modo ottimale una crisi informatica. Lo sviluppo di tale modello sarebbe particolarmente rilevante per le società pubbliche che sono soggette ai requisiti di reporting del Securities Exchange Act del 1934, poiché le aiuterebbe a conformarsi alle nuove regole proposte dalla Securities and Exchange Commission (SEC) nel 2022 in materia di gestione del rischio di sicurezza informatica, strategia, governance e pratiche di divulgazione degli incidenti (U.S. Securities and Exchange Commission, 2022).

Riconoscendo che le crisi di cybersecurity possono avere un impatto significativo sulle prestazioni finanziarie di un'azienda e, di conseguenza, anche sul rendimento degli investimenti degli investitori, la SEC ha proposto nuove regole che richiedono alle società quotate in borsa di divulgare periodicamente informazioni coerenti, comparabili e utili per le decisioni in merito alla loro gestione del rischio di cybersecurity, alla strategia e alle prassi di governance, nonché alla loro risposta agli incidenti di cybersecurity rilevanti e al ruolo di supervisione e all'esperienza di cybersecurity del loro consiglio di amministrazione e dei dirigenti. L'obiettivo finale di questa proposta è consentire agli investitori di valutare in modo più appropriato le prassi di gestione del rischio e di governance di un'azienda, in modo da informare meglio le loro decisioni di investimento e di voto.