LUISS

Corso di laurea in Strategic Management

Cattedra Metodi Quantitativi

# Rischio Cyber e Reputazione: il Ruolo dei Fattori Socioeconomici


Prof. Marco Pirra

RELATORE

Prof. Davide Angelucci

CORRELATORE

Julia Cavallaro 774021

CANDIDATO


Anno Accademico 2024/2025

**INDICE**

## INTRODUZIONE

Fino a trent'anni fa, era comune sentir parlare di spionaggio tradizionale: talpe, infiltrati, agenti che si introducevano fisicamente in ambienti riservati per sottrarre informazioni da rivendere o utilizzare per scopi illeciti. Oggi quel tipo di minaccia si è evoluta ed è diventata una delle principali sfide per la sicurezza di individui, aziende, Stati e dell'intera comunità globale (Word Bank, 2023). La figura della "spia" che si vedeva nei film di una volta e la figura dell'"hacker" ormai non esistono più. Si tratta di un concetto molto più ampio, ed esistono organizzazioni vere e proprie che lucrano sopra lo scambio di informazioni riservate per diffonderle o venderle creando confusione. Organizzazioni, che spesso vengono associate a gruppi terroristici, criminali, o hacker di alto livello. Le conseguenze di un attacco informatico possono avere un impatto significativo.

La sicurezza informatica è oggi parte integrante della sicurezza globale e dei singoli paesi. Ciò è dovuto alla crescente interconnessione digitale, che da un lato ha portato enormi vantaggi in termini di efficienza, innovazione e accesso alle informazioni, dall'altro ha creato nuove sfide. Tra queste, vi è la protezione dei dati (personali, nazionali e globali) da agenti malevoli, che possono sfruttarli per arrecare danni economici, operativi, giuridici e reputazionali in senso ampio. Dunque, in questo scenario, diventa essenziale non solo comprendere le dinamiche della cybersecurity, ma anche valutarne le implicazioni dirette, soprattutto sul piano reputazionale.

Questo elaborato intende offrire una visione chiara e completa del fenomeno, affrontandolo sia dal punto di vista teorico, sia dal punto di vista empirico. Nella prima parte della tesi verranno approfonditi i concetti di sicurezza informatica e reputazione, sia a livello aziendale che nazionale, attraverso l'analisi di casi concreti. Invece, la seconda parte verrà dedicata alla ricerca empirica basata sui dati del CISSM Cyber Events Database, che raccoglie eventi di attacchi informatici a livello mondiale dal 2014 al gennaio del 2025.

Il fine ultimo è comprendere in che modo la numerosità e la distribuzione degli attacchi cyber possano influenzare la reputazione dei paesi, con eventuali ripercussioni di natura

economica e geopolitica. A tal fine, la ricerca risponde alla seguente domanda: “In che misura i cyber attacchi incidono sulla reputazione aziendale e sulla percezione internazionale di un paese?”

Per rispondere, sono state formulate e testate le seguenti tre ipotesi:
H1: I paesi con reddito più elevato registrano un numero maggiore di attacchi cyber.
H2: La frequenza degli eventi varia significativamente tra settore e nel corso degli anni.
H3: Gli attacchi informatici influenzano la performance economica e di conseguenza la reputazione di un paese.

Pertanto, la tesi sarà sviluppata in tre capitoli. Nel primo capitolo viene presentato il tema della cybersecurity, analizzandone l’evoluzione storica, le principali conseguenze, le sfide per le organizzazioni e gli strumenti normatici oggi disponibili. Mentre, il secondo capitolo affronta il tema della reputazione, sia a livello aziendale, sia a livello nazionale, ponendo le basi per l’analisi empirica. Successivamente, nell’ultimo capitolo, viene presentata la ricerca condotta con il software SPSS, vengono elaborati i dati e le ipotesi formulate, per arrivare alle conclusioni finali, accompagnate da una discussione critica e dal riconoscimento delle limitazioni dello studio.

# CAPITOLO 1 – CYBERSECURITY: EVOLUZIONE, RISCHI E RILEVANZA STRATEGICA

La "sicurezza" è il bisogno più fondamentale di ogni società e costituisce il fattore più importante della vita sociale. Nel corso della storia, l'uomo ha sempre cercato condizioni sicure e prive di rischio, dando così origine alle prime istituzioni sociali. Di conseguenza, la sicurezza è considerata una delle colonne portanti della vita collettiva e, in sua assenza, il caos diventa inevitabile. Non è quindi sorprendente che molti filosofi, come Hobbes e Machiavelli, abbiano posto la sicurezza come valore fondamentale nei loro pensieri, arrivando persino a giustificare forme di governo più autoritarie, pur di garantire ordine e sicurezza nella società. [1]

A causa della crescente digitalizzazione ed interconnessione, il concetto di sicurezza ha assunto significati più ampi e complessi. In particolare, l'avvento della rivoluzione digitale e la diffusione di Internet hanno trasformato profondamente le modalità di comunicazione, di interazione sociale e di gestione dell'informazione, introducendo nuove forme di vulnerabilità. Infatti, le nuove tecnologie stanno portando molti benefici, ma, allo stesso tempo, è necessario contenere i rischi che ciò potrebbe causare (Control Risks, 2024). È in questo contesto che nasce il cyberspazio e la necessità di introdurre la sicurezza informatica. Infatti, ormai si sono creati due mondi in cui circolano e si sviluppano informazioni di vario genere: lo spazio terrestre e il cyberspazio. Il primo riguarda quello umano, al quale siamo abituati; mentre, il secondo rappresenta una nuova forma di spazio, creatasi recentemente, che contiene tutti i dati immagazzinati online, che si muovono velocemente, che possono essere reperiti in più località geografiche contemporaneamente e, soprattutto, possono essere ottenuti da più utenti nello stesso momento.

Ad oggi, la cybersecurity non riguarda più soltanto la protezione dei sistemi informatici da virus o intrusioni, ma è diventata una condizione essenziale per la stabilità sociale, economica e politica di una nazione. La forte interconnessione nel mondo, porta a trasformare ogni singola minaccia digitale ad un evento molto più ampio e catastrofico che può avere ripercussioni reali e tangibili sulla vita delle persone e sul funzionamento

[1] Kazemi, A., Kalhornia Golkar, M., & Lajmiri, S. (2023). *Origins of cyber security: Short report*. *International Journal of Reliability, Risk and Safety: Theory and Application*, *6*(2), 77–83.

delle istituzioni. Per questo motivo, la sicurezza informatica si è evoluta nel tempo ed è diventata priorità strategica a livello globale. Governi, aziende e organizzazioni internazionali stanno investendo sempre più risorse significative per proteggere infrastrutture critiche, dati riservati e reti di comunicazione. Allo stesso tempo, la crescente complessità degli attacchi, sempre più mirati, precisi e sofisticati, ha reso evidente l'insufficienza di approcci tradizioni alla sicurezza digitale e la necessità di spendere più risorse in sistemi capaci di rilevare, rispondere e adattarsi rapidamente alle minacce. [2]

### 1.1 Evoluzione storica della cybersecurity

La storia del mondo cyber è in continua evoluzione e non è così recente come può sembrare. Infatti, si possono distinguere diverse fasi, che corrispondono sostanzialmente all'evoluzione delle tecnologie negli anni: prima di Internet, dopo la diffusione dei computer e delle reti, e l'era dell'Intelligenza Artificiale e Machine Learning.

Prima degli anni '60, commettere un cybercrimine risultava molto più difficile. In assenza delle reti di comunicazione e di Internet, per poter accedere ai dati di un computer, bisognava avere l'accesso fisico ad esso, commettendo quindi una violazione di proprietà privata, ma non di "hackeraggio" come si intende ad oggi. In aggiunta, durante la Seconda Guerra Mondiale, le prime forme di sicurezza informatica avevano lo scopo di proteggere informazioni classificate militari e governative, portando allo sviluppo della macchina Enigma, tramite lavori pionieristici del campo della cifratura e crittografia. [3]

Dagli anni '60 in poi, furono sviluppate le prime reti di comunicazione e sistemi che permettevano la trasmissione di dati a distanza, come ARPANET, il progetto dell'ARPA (Advanced Research Project Agency), che permise lo scambio di pacchetti di dati e gettò le basi del futuro cyberspazio.

Negli anni '70 e '80, iniziarono a emergere i primi problemi di sicurezza, collegati alla diffusione del primo virus informatico: Creeper. Quest'ultimo non era stato programmato con intenti dannosi, ma era semplicemente un programma in grado di autoreplicarsi tra

[2] Mallick, M. A. I., & Nath, R. (2024). *Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments*. World Scientific News

[3] Brown, R., Bailey, C., Hunt, S., Tarbitten, P., Finch, C., & Forcythe-Reid, E. (2024). *Technological advancements and hacker ingenuity: The evolution of cyber security and a zero trust model*. *Science in Parliament, 80*(2), 12–15.

computer, mostrando il seguente messaggio: “Sono Creeper. Acchiappami se ci riesci”. Come conseguenza, venne creato il primo software antivirus, “Reaper”, ovvero un programma che era in grado di individuare ed eliminare il virus. Questa sfida tra malware e anti-malware segnò l’inizio di una lunga “guerra informatica”.

Contemporaneamente lo sviluppo di Internet e la crescente diffusione di computer e reti portarono ad un utilizzo sempre più esteso delle tecnologie digitali e, di conseguenza, a rischi informatici sempre più significativi. Se inizialmente le informazioni presenti in rete erano limitate e frammentarie, con il tempo si cominciò a registrare una mole sempre più ampia di dati, spesso contenenti informazioni sensibili, inclusi anche dati di natura governativa. In questo periodo, si assistette ai primi casi eclatanti di hacking e furti di informazioni, che ebbero come conseguenza la nascita dell’industria antivirus, [4] e venne coniato il termine “computer virus” nel 1983. [5]

Di questi casi ce ne fu uno in particolare che cambiò le cose in maniera drastica: il Morrison Worm del 1988. Si trattava di un *worm*, ovvero un’applicazione in grado di replicarsi molto velocemente attraverso Internet, lanciato inizialmente come esperimento accademico, ma che finì fuori controllo, infettando circa centomila computer allora interconnessi.[6] L’impatto di questo incidente, i cui danni inizialmente vennero stimati a 100 mila dollari, per poi diventare milioni, funse come campanello d’allarme: le aziende informatiche ed anche i governi si resero conto che non si trattava più di un una rete libera, sicura e neutrale, ma un sistema con vulnerabilità potenzialmente dannose, che rendevano urgente lo sviluppo di adeguate misure di protezione.[7] Per far fronte a questi cybercrimini, poco dopo venne fondato il CERT (Computer Emergency Response Team) e istituito un protocollo crittografico molto valido, il DES (Data Ecryption Standard), adottato su larga scala per la protezione dei dati e prevenzione di attacchi e furti.

---

[4] NordVPN. (n.d.). *La storia della cybersecurity*. https://www.nordvpn.com/it/blog/la-storia-della-cybersecurity/

[5] Brown, R., Bailey, C., Hunt, S., Tarbitten, P., Finch, C., & Forcythe-Reid, E. (2024). *Technological advancements and hacker ingenuity: The evolution of cyber security and a zero trust model*. *Science in Parliament, 80*(2), 12–15.

[6] **ICE Media (2021, maggio 12).** *Trent’anni di insicurezza digitale (1988–2018): che cosa ci riserva il prossimo decennio?* Agenda Digitale. https://www.agendadigitale.eu/sicurezza/trentanni-di-insicurezza-digitale-1988-2018-che-ci-riserva-il-prossimo-decennio/

[7] Maryville University Online. (2024, luglio 24). *The history of cybersecurity*. https://online.maryville.edu/blog/history-of-cybersecurity/

Con gli anni ’90, l’avvento del World Wide Web e la diffusione di massa di Internet, aprirono una nuova era per la cybersecurity. Se da un lato l’interconnessione globale portava enormi opportunità, dall’altro emersero minacce sempre più sofisticate e cybercriminali motivati da profitto. In questo decennio sono stati registrati attacchi e malware divenuti celebri, come il virus Melissa del 1999, che si diffuse via e-mail causando circa 80 milioni di dollari di danni. [8] Contestualmente, come dopo il Morrison Worm, i governi si resero conto che bisognava intervenire in modo più deciso, emanando le prime normative sulla sicurezza (ad esempio, le linee guida BS 7799 ed ISO 27001), e si affermò l’idea che la sicurezza dovesse essere gestita in modo sistematico dalle organizzazioni.

Gli anni 2000 furono segnati da una esplosione di attacchi informatici su scala globale. I virus e i worm divennero sempre più veloci e distruttivi, famoso il “Love bug” virus, e i worm “Code Red” e “SQL Slammer” che sfruttarono vulnerabilità dei software diffusi, mandando in crisi server e reti in tutto il mondo. Questi eventi spinsero le aziende a rafforzare ulteriormente le misure di sicurezza e i governi ad introdurre leggi più stringenti. Ad esempio, nel 2004, gli Stati Uniti vararono il *Computer Fraud and Abuse Act* e a livello internazionale si discusse della Convenzione di Budapest (2001) sul cybercrimine per perseguire i crimini informatici oltre confine.

Nel decennio 2010-2020 la cybersecurity è divenuta una priorità strategica conclamata. Da un lato, la massiccia adozione del cloud computing e dei social network ha ampliato la superficie di attacco, richiedendo nuove soluzioni di sicurezza; dall’altro, si è assistito ad una crescita di attacchi *state-sponsored* (i cui mandanti erano gli Stati stessi o gruppi APT*[9]) ed episodi di cyber warfare e spionaggio industriale senza precedenti. Alcuni esempi molto noti che hanno segnalato l’ingresso del cyberspazio del campo geopolitico sono vari. Tra questi osserviamo il noto malware “Stuxnet” nel 2010 avrebbe distrutto numerose centrifughe nell’impianto di arricchimento in Iran, facendole bruciare. [10] Non

[8] Federal Bureau of Investigation. (2019, March 25). *The Melissa virus: FBI marks 20th anniversary*. FBI. https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519

[9] *Advanced Persistent Threat

[10] Trellix. (n.d.). *What Is Stuxnet?* https://www.trellix.com/security-awareness/ransomware/what-is-stuxnet/

da meno anche i casi di intrusione ai danni di Sony Pictures nel 2014, episodio più eclatante di hacking nel settore privato, e soprattutto le interferenze informatiche nelle elezioni presidenziali degli Stati Uniti nel 2016 da parte della Russia. [11] Nel frattempo, esplose anche il fenomeno del ransomware che attaccava aziende e infrastrutture, cifrando dati e chiedendo riscatti, segnando un punto di svolta nella percezione delle minacce informatiche a livello globale.

Arrivando all'era contemporanea, anni 2020 e oltre, la disciplina della sicurezza informatica continua ad evolvere in risposta a minacce sempre più sofisticate e alla gestione di infiniti dati. Probabilmente si tratta dell'"era d'oro" della cybersecurity e sono due le grandi innovazioni protagoniste di questo periodo: l'Intelligenza Artificiale e il Machine Learning. Si tratta di due tecnologie che presentano un paradosso: da un lato, rappresentano un potente alleato nella prevenzione e nel contrasto delle minacce informatiche; dall'altro, aprono la strada a nuovi rischi, poiché possono essere sfruttate per sviluppare attacchi sempre più elaborati e difficili da rilevare. Infatti, l'IA consente agli aggressori di automatizzare attacchi mirati come lo *spear phishing*, creare *deepfake* realistici e individuare vulnerabilità nei software su ampia scala. In aggiunta, i progressi nel calcolo quantistico minacciano di rendere obsoleti gli attuali sistemi di crittografia, e per questa ragione, si sta lavorando sullo sviluppo di algoritmi di crittografia resistenti al quantistico, progettati per resistere alle vulnerabilità crittografiche dei computer, garantendo la sicurezza continua dei dati sensibili. [12]
La superficie di attacco è enormemente cresciuta anche a causa dell'Internt of Things (infiniti dispositivi IoT connessi ad Internet che necessitano protezione) e all'interconnessione digitale globale.
Pertanto, si è passati dalla gestione di un numero limitato di dati e minacce contenute, a un contesto di interconnessione globale, caratterizzato da una quantità infinita di dati, minacce complesse e una capacità di intercettazione notevolmente ampliata. Dunque, per ogni innovazione tecnologica che porta benefici, emergono nuove vulnerabilità da

[11] **Federal Bureau of Investigation. (2018, July 13).** *Russian interference in 2016 U.S. elections*. FBI. https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections
[12] Heiding, F. (2025, maggio 13). *72% of cyber leaders say risks are rising. Here's how states and businesses are responding*. World Economic Forum. https://www.weforum.org/stories/2025/05/cybersecurity-cyber-risk-national-policy/

mitigare.[13] Come sottolinea il Professore ed esperto in materia Michele Colojanni, nella sua opera "*Oltre trent'anni di (in)sicurezze informatica*", l'esperienza accumulata in decenni di evoluzione digitale ci ha trasmesso una verità indiscutibile: "tutto ciò che si basa sul software è insicuro". Eppure, si continua ad affidare allo stesso software il controllo del mondo, tra cui il controllo di infrastrutture, sistemi critici e della società del suo complesso. [14]

Questo scenario ha reso necessaria la cooperazione da parte di tutti i paesi, creando un senso di responsabilità collettiva per fronteggiare una minaccia che comporta costi enormi: solo nel 2024 è stato registrato un danno globale di 9,4 trilioni di dollari.[15] Pertanto, oggi, non è più possibile sottovalutare il problema né considerarlo un semplice problema tecnico legato all'IT, perché la cybersicurezza è ormai una responsabilità condivisa che riguarda tutti: singoli individui, piccole medie imprese, grandi aziende e organizzazioni, istituzioni e la comunità globale.

## 1.2 Definizione di cybersecurity, concetti fondamentali e differenza tra information security e cybersecurity

Nonostante il termine "cybersecurity" sia di uso comune, è importante definirlo con precisione e distinguerlo da concetti affini come "information security". Il termine information security si riferisce tradizionalmente alla protezione delle informazioni e dei sistemi informatici da accessi non autorizzati, uso o manipolazione illecite, al fine di garantire i principi di riservatezza, integrità e disponibilità dei dati. Questa classifica si riferisce al modello Triade CIA (Confidentiality, Integrity, Availability) e rappresenta da decenni le fondamenta della sicurezza delle informazioni. [16] Per capire al meglio questi tre termini, si possono considerare alcuni esempi pratici: la riservatezza può essere garantita attraverso la crittografia dei dati per impedirne la lettura da parte di estranei; l'integrità si assicura con firme digitali o codici di controllo specifici che verificano che i

[13] BlueVoyant. (2025). *Cybercrime: History, Global Impact & Protective Measures*. https://www.bluevoyant.com/knowledge-center/cybercrime-history-global-impact-protective-measures-2022

[14] Colajanni, M. (2018, 19 novembre). *Trent'anni di insicurezza digitale (1988-2018): che ci riserva il prossimo decennio?*Agenda Digitale. https://www.agendadigitale.eu/sicurezza/trentanni-di-insicurezza-digitale-1988-2018-che-ci-riserva-il-prossimo-decennio/

[15] Mallick, M. A. I., & Nath, R. (2024). *Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments*. World Scientific News

[16] European Union Agency for Network and Information Security. (2017). *ENISA overview of cybersecurity and related terminology* (Version 1). https://www.enisa.europa.eu/

dati non siano stati modificati; infine, la disponibilità viene tutelata con backup e sistemi duplicati per garantire l'accesso ai dati anche in caso di problemi o attacchi.

Come è stato evidenziato nel paragrafo precedente, il termine cybersecurity è emerso nell'ultimo ventennio, ed è considerato come un ampliamento del campo dell'information security. Secondo il NIST, ovvero il National Institute of Standards and Technology, la cybersecurity è l'"*abilità di proteggere o difendere l'uso del cyberspazio dagli attacchi informatici*". [17] In altre parole, la cybersecurity riguarda tutte le misure necessarie per proteggere l'ecosistema digitale, tra cui reti, sistemi, software, dispositivi, programmi e dati, dalle minacce cyber. Per avere una definizione più completa, si considera anche la visione omnicomprensiva dell'agenzia Europea per la cybersicurezza ENISA, che definisce la cybersecurity come "*tutte le attività necessarie a proteggere il cyberspazio, i suoi utenti e le persone potenzialmente impattate dalle minacce cyber*". Ciò evidenzia che la cybersecurity copre ulteriori aspetti rispetto alla mera protezione dei dati, includendo anche la sicurezza delle reti, dei sistemi industriali, dei servizi digitali e più in generale tutto ciò che rientra del cyberspazio. Pertanto, oltre alla Triade CIA, negli anni sono stati aggiunti altri attributi e principi fondamentali per descrivere la sicurezza nello spazio cyber. Tra questi emergono l'autenticità (autenticazione dell'identità delle parti e dei dati), il "non ripudio" (per supportare la sicurezza delle informazioni), la tracciabilità (capacità di attribuire le azioni ad un soggetto), l'affidabilità, la manutenibilità (per sistemi tangibili, informazioni e reti), robustezza, sopravvivenza e la resilienza (per supportare la dinamicità).[18] Questi concetti più estesi rappresentano la dinamicità e i continui cambiamenti che sono avvenuti nell'ambito tecnologico e digitale in questi anni, rendendo necessario un ampliamento della dottrina. A sua volta, la cybersecurity odierna non si limita più a prevenire violazioni, ma comprende anche la capacità di rilevare, rispondere e recuperare dagli incidenti.

Quindi, la differenza tra queste due discipline, che possono sembrare simili, in realtà è vasta. L'information security ha un campo anch'essa molto ampio, occupandosi di sicurezza delle informazioni in qualunque forma (digitale o meno) e includendo anche

[17] National Institute of Standards and Technology. (2025, 3 luglio). *Cybersecurity*. In *NIST Computer Security Resource Center Glossary*. https://csrc.nist.gov/glossary/term/cyber_security

[18] European Union Agency for Network and Information Security. (2017). *ENISA overview of cybersecurity and related terminology* (Version 1). https://www.enisa.europa.eu/

aspetti tangibili come gli archivi cartacei, controlli d'accesso ecc. Invece, la cybersecurity si focalizza sull'ambiente digitale (cyber) e sulle tecnologie ICT (Tecnologie dell'Informazione e della Comunicazione). [19] In pratica, nelle organizzazioni odierne i due termini convergono: garantire la sicurezza delle informazioni implica necessariamente misure di cybersecurity, dato che ormai la maggior parte di informazioni risiede e transita su sistemi digitali.

Per concludere, si può dunque affermare che la cybersecurity corrisponde alla sicurezza dei dati e delle informazioni nell'era di Internet e comprende la prevenzione, il rilevamento e la risposta ad attacchi informativi, con l'obiettivo ultimo di proteggere dati, sistemi e persone dagli impatti negativi del mondo digitale.

### 1.3 Tipologie di attacchi informatici e principali vulnerabilità

Il panorama delle minacce cyber è estremamente vario e in continua evoluzione. Si possono però classificare le tipologie di attacchi informatici in alcune grandi categorie, tenendo presente che spesso gli attacchi reali combinano più tecniche.

Secondo l'ultimo rapporto ENISA sulle minacce (Threat Landscape 2024)[20], le principali categorie di attacchi attualmente utilizzate sono otto, ed includono:

- Malware: si tratta di un software malevolo di vario tipo (*virus, worm, trojan, ransomware, spyware*, *zero-day* ecc.) usato per infiltrarsi nei sistemi e compiere azioni dannose (ad esempio cancellare o cifrare dati, rubare informazioni, compromettere il dispositivo). Più nel dettaglio, un ransomware cifra i file della vittima e richiedere un riscatto per ripristinarli, mentre uno *spyware* può registrare di nascosto tutto ciò che l'utente digita, sottraendo password e dati sensibili. I malware restano una minaccia primaria e in costante aumento. Del resto, basti pensare che ogni giorno vengono scoperte migliaia di nuovi campioni di malware. [21]

[19] GeeksforGeeks. (n.d.). *Difference between cyber security and information security*. https://www.geeksforgeeks.org/difference-between-cyber-security-and-information-security/
[20] European Union Agency for Cybersecurity. (2024, September). *ENISA threat landscape 2024: July 2023 to June 2024*. Publications Office of the European Union. https://doi.org/10.2824/0710888
[21] https://nordvpn.com/it/blog/la-storia-della-cybersecurity/

- Ransomware: è un attacco informatico in cui gli hacker prendono il controllo di informazioni sensibili di una vittima, chiedendo un riscatto in cambio del loro ripristino o per evitarne la divulgazione pubblica. Questa definizione consente di cogliere l'evoluzione del fenomeno, caratterizzato dall'utilizzo crescente di diverse tecniche di estorsione e da obiettivi che non si limitano solo al guadagno economico. Negli ultimi anni, il ransomware si è confermato come una delle principali minacce, con numerosi episodi di grande impatto, ampliamente riportati dai media.
- Social Engineering: sono attacchi che sfruttano l'inganno psicologico degli utenti per ottenere accessi o informazioni. Il più noto è il *phishing*, in cui l'aggressore sfrutta vari canali di comunicazione (e-mail, messaggi istantanei, finestre pop-up o pagine web) [22] fingendosi un'entità fidata per indurre la vittima a rivelare credenziali o cliccare link infetti. Esistono ulteriori varianti, come lo "*spear phishing*" che tendenzialmente è mirato ad una persona/azienda specifica, e il "*whaling*", mirato più ai dirigenti. In aggiunta, nel social engineering rientra anche il "*pretexting*", ovvero la costruzione di un pretesto per ottenere informazioni, e l'inganno telefonico, anche chiamato "*vishing*". Questi attacchi puntano sul fattore umano, considerato spesso l'anello debole della sicurezza.
- Furti e violazione di dati: il GDPR (Regolamento Generale sulla Protezione dei Dati) definisce una violazione di dati come qualsiasi violazione della sicurezza che comporti la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso illecito a dati personali trasmessi, archiviati o comunque trattati. Da un punto di vista tecnico, le violazioni di dati possono essere distinte in due categorie: *data breaches* e *data leak*. Sebbene i due termini vengano utilizzati come sinonimi, descrivono due concetti differenti. Infatti, un *data breach* è un attacco informatico intenzionale, condotto da un cybercriminale con l'obiettivo di ottenere l'accesso non autorizzato ad un sistema o organizzazione e diffondere dati sensibili, riservati o protetti. Mentre, un *data leak* è un evento accidentale che porta alla perdita o all'esposizione non intenzionale di dati sensibili o protetti. I *data breach* sono all'ordine del giorno e spesso sono legati

[22] Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (Year). *Cybersecurity threats and vulnerabilities: Systematic mapping study*.

anche ad errori di configurazione o vulnerabilità non risolte, come per esempio, esposizioni di database online senza password, o vulnerabilità sfruttate per estrarre elenchi di utenti e password.

- Attacchi contro la disponibilità: questo tipo di attacco mira a rendere un sistema o un servizio inaccessibile agli utenti legittimi.[23] Il più comune è l'attacco DoS (Denial of Service) e la sua forma distribuita DDoS (Distributed Denial of Service), in cui una vasta quantità di dispositivi compromessi inonda di traffico malevolo un server o un sito web, mandando in tilt e impedendone l'accesso. [24] Nel rapporto di ENISA, i DDoS vengono indicati come una delle minacce più elevate insieme al ransomware. Il motivo principale è che gli attacchi alla disponibilità possono anche colpire infrastrutture critiche: ad esempio, bloccare server di controllo industriale per interrompere forniture di servizi essenziali generando caos.
- Attacchi alla supply chain digitale: riguardano l'infiltrazione in componenti di terze parti per colpire a cascata molte vittime e solitamente consiste in una combinazione di almeno due attacchi. Poiché un attacco sia classificato come *supply chain attack*, sia il fornitore che il cliente devono essere bersagli dell'azione. Un esempio cardine è il caso SolarWinds del 2020, che verrà approfonditi in seguito, in cui un aggiornamento software IT infettò migliaia di organizzazioni, mettendo in luce il potenziale di questo tipo di attacchi.
- Disinformazione e manipolazione informativa: si riferisce ad un comportamento, per lo più non illegale, che minaccia o ha il potenziale di influenzare negativamente valori, procedure e processi politici. Un esempio è la diffusione di fake news o semplici alterazioni di informazioni che possono essere accompagnati da attacchi tecnici, causando confusione nell'opinione pubblica, perdita di fiducia nelle istituzioni e polarizzazione sociale.

Nel grafico seguente vengono rappresentate in modo più chiaro le principali tipologie di attacco e la loro frequenza. Nel periodo compreso tra luglio 2023 e giugno 2024, i ransomware (25,79%) e gli attacchi DDoS (41,1%) sono risultate le forme più segnalate,

[23] Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (Year). *Cybersecurity threats and vulnerabilities: Systematic mapping study*.
[24] https://nordvpn.com/it/blog/la-storia-della-cybersecurity/

seguite dalle violazioni di dati (19,01%). Poiché il report ENISA si basa esclusivamente su fonti pubbliche disponibili, non sempre è possibile ottenere un quadro esaustivo e completo, in quanto molti episodi possono risultare parzialmente documentati ed altri non sempre vengono classificati in una categoria precisa.

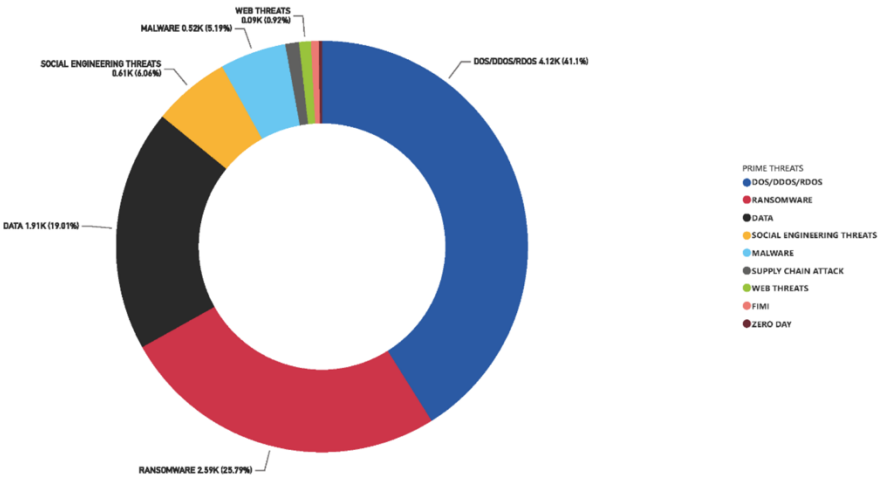



Figura 1: Tipologie di attacchi cyber registrati tra luglio 2023 e giugno 2024. Fonte: ENISA 2024

Pertanto, i cyber aggressori spesso utilizzano una combinazione di questi metodi per raggiungere i loro obiettivi, e le loro motivazioni possono variare notevolmente, includendo ragioni ideologiche, politiche, finanziarie o semplicemente il desiderio di causare caos e disordini come simbolo di protesta.

Oltre alle tipologie di attacco, è cruciale considerare le vulnerabilità principali che gli attori malevoli sfruttano. Una vulnerabilità è una debolezza o falla in un sistema (software, hardware, processo o elemento umano) che può essere sfruttata per violarne la sicurezza, e molto spesso viene definita come “il tallone d’Achille di un’applicazione o un software”. Queste vulnerabilità possono essere il risultato delle seguenti azioni:

- Bug nei software: sono spesso degli errori di programmazione, che se non corretti in tempo, permettono ad un hacker di arrivare ad ottenere accessi non autorizzati. Inoltre, molti di questi bug vengono registrati e resi pubblici, e se non aggiornati

in tempo, rimangono esposti e facilmente sfruttabili da altri potenziali attaccanti. [25]

- Configurazioni errate: avvengono quando parametri di sicurezza sono stati impostati in modo errato e rappresentano un varco di entrata facile per gli hacker. Pertanto, molti *data breach* avvengono perché i database o i server vengono lasciati accessibili online senza adeguate protezioni.
- Credenziali deboli o compromesse: quando le password sono deboli, riutilizzate su più piattaforme o lasciate di default. Anche la mancanza dell'autenticazione a due fattori è vista come una possibile vulnerabilità, poiché facilita l'accesso e l'uso fraudolento di credenziali rubate.
- Vulnerabilità umane: l'errore umano o la scarsa consapevolezza sono molto comuni e vengono sfruttate dal *social engineering* e dal *phishing.* Per esempio, un dipendente che clicca su un allegato infetto o fornisce informazioni sensibili al telefono può compromettere l'efficacia anche delle difese tecniche più robuste. Per questo motivo, la formazione degli utenti e la cultura della sicurezza sono considerate parte integrante della gestione della vulnerabilità e della strategia complessiva di sicurezza.

Dunque, l'hacker per avere successo, deve prima individuare una vulnerabilità da sfruttare, che può essere più tecnica, di configurazione o umana, e scegliere una tipologia di attacco adatto allo scopo. Le organizzazioni devono quindi lavorare sia sulla riduzione delle vulnerabilità, sia sulla difesa tecnica, munendosi di sistemi di sicurezza validi, come antivirus aggiornati, autenticazione a più fattori e strumenti monitoraggio continuo.[26]

In questo contesto, è fondamentale considerare anche l'ampliamento della superficie di attacco informatico, ovvero l'aumento dei punti potenzialmente esposti a minacce, dovuto soprattutto alla crescente digitalizzazione e alla diffusione di dispositivi connessi.

## 1.4 Conseguenze degli attacchi informatici: impatti economici, operativi, legali e reputazionali

[25] Keeper Security. (2023, dicembre 27). *Common types of cybersecurity vulnerabilities*. https://www.keepersecurity.com/blog/2023/12/27/common-types-of-cybersecurity-vulnerabilities/
[26] https://www.youtube.com/watch?v=gwjW8Gy4Q-0

Nei paragrafi precedenti si è fatto riferimento agli attacchi informatici, senza tuttavia approfondire la reale portata e gravità. Oltre al semplice inconveniente tecnico, fenomeni come il furto di dati, manipolazione di informazioni, l'interruzione di servizi essenziali o l'utilizzo di Internet come mezzo di minaccia e intimidazione rientrano a pieno titolo tra i crimini informatici. Con l'importanza sempre più crescente delle infrastrutture digitali e il costante abbassamento delle barriere d'accesso per i potenziali aggressori, la sicurezza informatica è divenuta una preoccupazione di primo piano a livello globale, come dimostra l'aumento del 61,5% degli attacchi cyber nel mondo tra il 2018 e il 2023. [27]

Dunque, è fondamentale comprendere le conseguenze di un attacco informatico, ed andare oltre al mero danno informatico immediato. Gli attacchi più gravi possono infatti avere effetti significativi su una vasta gamma di entità, dalle singole aziende fino alle collettività nazionali. Pertanto, come è stato messo a fuoco precedentemente, rilevare, prevenire e contrastare questo tipo di crimine presenta sfide uniche per le forze dell'ordine ed i governi, richiedendo un approccio sempre più coordinato e multidimensionale.

Alcuni di questi effetti, si possono individuare nel grafico sottostante. La Figura 2 illustra le conseguenze più frequenti degli incidenti informatici a livello mondiale nel 2023, che vanno ben oltre la perdita immediata di dati. Le ripercussioni possono includere interruzioni operative, danni reputazionali, perdita di competitività e sanzioni normative, danneggiando la reputazione e la stabilità di un intero paese. Più nel dettaglio, nelle conseguenze relative ad interruzioni operative, bisogna evidenziare il fatto che molte di queste possono avere a che fare con le interruzioni di infrastrutture critiche come reti elettriche, ospedali, fondi di acqua e sistemi di trasporto, causando gravi disagi e panico su larga scala. [28]

[27] Leonardi, A. (2024, 25 gennaio). *Attacchi informatici: conseguenze economiche e strategie di difesa*. Cybersecurity360. https://www.cybersecurity360.it/soluzioni-aziendali/attacchi-informatici-conseguenze-economiche-strategie-difesa-business/

[28] Ɨikhar, S. (2024). *Cyberterrorism as a global threat: A review on repercussions and countermeasures*. *PeerJ Computer Science, 10*, e1772. https://doi.org/10.7717/peerj-cs.1772

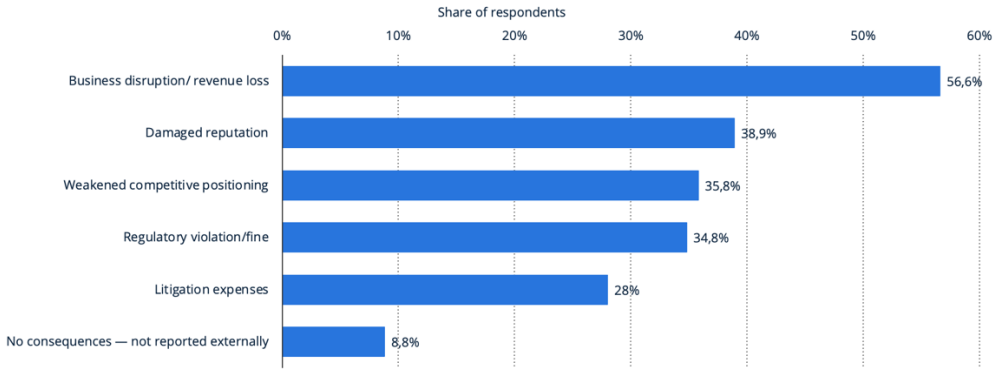



Figura 2: Conseguenze più comuni delle violazioni di dati negli enti a livello globale nel 2023. Fonte: Statista

Dunque, per rendere l'analisi più chiara e strutturata, tali conseguenze sono state suddivise in quattro aree di impatto: economico, operativo, giuridico e reputazionale.

### 1.4.1 Impatto economico

Una delle prime conseguenze di un attacco informatico riguarda il danno economico diretto. Questa categoria include tutti i costi finanziari immediati subiti dall'organizzazione vittima della violazione. In particolar modo, la perdita economica comprende vari tipi di spese, tra cui: costi di risposta e ripristino, perdite economiche dirette e riscatti pagati. Le prime fanno riferimento alle spese per le indagini, il rispristino dei dati e dei sistemi compromessi, oltre al miglioramento delle misure di sicurezza dopo l'incidente. Le seconde vengono rappresentate dai mancati ricavi dovuti all'interruzione delle attività operative durante e dopo l'attacco; mentre, spesso, per riottenere l'accesso alle informazioni o ai sistemi critici, molte aziende sono costrette a pagare un riscatto, perdendo altri soldi.

Recenti ricerche quantificano in modo significativo l'impatto finanziario medio di una violazione. Secondo il rapporto Cost of Data Breach 2024 di IBM, il costo medio globale di una violazione di dati ha raggiunto 4,88 miliardi di dollari nel 2024, con un incremento del 10% rispetto all'anno precedente. [29] Si tratta del valore più alto mai registrato fino ad ora, segno che gli incidenti informatici stanno diventando sempre più onerosi da gestire.

[29] IBM. (2024, July 30). *IBM report: Escalating data breach disruption pushes costs to new highs*. IBM Newsroom. https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs

Come dimostra il grafico sottostante, il costo medio di un *data breach* è aumentato in modo costante nell'ultimo decennio.

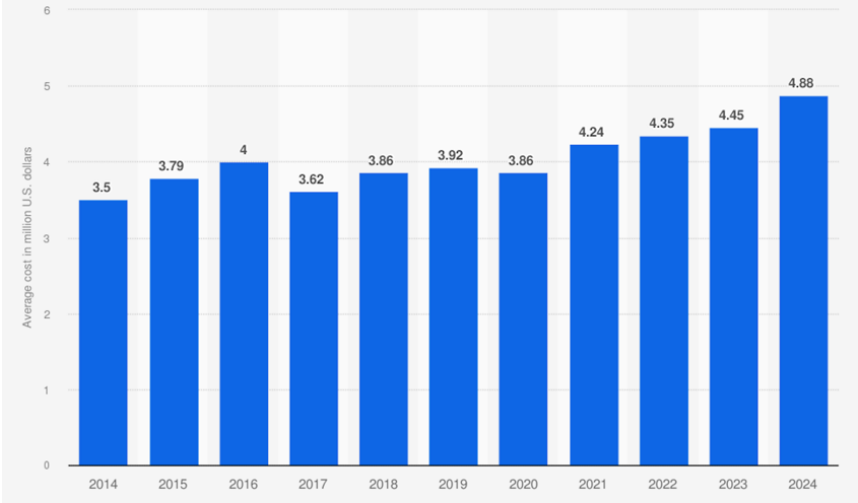



Figure 3: Costo medio di un *data breach* a livello mondiale, 2014-2014 (milioni US$). Fonte: Statista

Naturalmente, questa cifra media nasconde differenze notevoli, in quanto il costo effettivo di un attacco varia in base alla gravità dell'incidente e alle dimensioni dell'organizzazione colpita. Infatti, violazioni di entità minori possono avere impatti economici relativamente contenuti e attacchi gravi o rivolti a grandi enti comportano perdite finanziarie decisamente più elevate.

Le informazioni della seguente tabella dimostrano come comparti ad alta intensità di dati sensibili, come sanità e finanza, registrano un costo medio nettamente superiore alla media globale, con picchi che superano i 9 milioni di dollari. Altri settori, come l'istruzione o l'intrattenimento, presentano invece valori inferiori, pur rimanendo comunque esposti a perdite considerevoli.

Queste differenze, che verranno analizzati nel dettaglio più avanti, evidenziano l'importanza di strategie di sicurezza calibrate sul contesto operativo e sul livello di rischio specifico di ciascun settore.

| Characteristic | May 2020 - Mar 2021 | Mar 2021 - Mar 2022 | Mar 2022 -Mar 2023 | Mar 2023 -Feb 2024 |
|---|---|---|---|---|
| Healthcare | 9.23 | 10.1 | 10.93 | 9.77 |
| Financial | 5.72 | 5.97 | 5.9 | 6.08 |
| Pharmaceuticals | 5.04 | 5.01 | 4.82 | 5.1 |
| Technology | 4.88 | 4.97 | 4.66 | 5.45 |
| Energy | 4.65 | 4.72 | 4.78 | 5.29 |
| Professional services | 4.65 | 4.7 | 4.47 | 5.08 |
| Industrial | 4.24 | 4.47 | 4.73 | 5.56 |
| Global average | 4.24 | 4.35 | 4.45 | 4.88 |
| Research | 3.6 | 3.88 | 3.63 | 3.54 |
| Education | 3.79 | 3.86 | 3.65 | 3.5 |
| Consumer | 3.7 | 3.86 | 3.8 | 3.91 |
| Entertainment | 3.8 | 3.83 | 3.62 | 4.09 |
| Communications | 3.62 | 3.62 | 3.9 | 4.09 |
| Transportation | 3.75 | 3.59 | 4.18 | 4.43 |
| Retail | 3.27 | 3.28 | 2.96 | 3.48 |
| Media | 3.17 | 3.15 | 3.58 | 3.94 |
| Hospitality | 3.03 | 2.94 | 3.36 | 3.82 |
| Public sector | 1.93 | 2.07 | 2.6 | 2.55 |

Figura 4: Costo medio di una violazione di dati a livello mondiale per settore, maggio 2020 - febbraio 2024 (milioni US$). Fonte: Statista

### 1.4.2 Impatto operativo

L'impatto operativo si riferisce all'effetto immediato sull'operatività dell'azienda. Un attacco grave può causare l'interruzione di servizi e processi produttivi, l'indisponibilità di sistemi e dati critici, con conseguente fermo delle attività. Ad esempio, un ransomware che blocca i database aziendali può interrompere per giorni la capacità di evadere ordini, gestire transazioni o fornire servizi ai clienti. In tempi recenti sono diventati sempre più comuni anche gli attacchi alla supply chain, in cui i criminali colpiscono fornitori terzi per propagare il danno a molte aziende nello stesso momento.

Secondo un rapporto pubblicato da Cowbell, tra il 2021 e il 2023 questi attacchi sono aumentati del 431%, e continueranno ad aumentare in modo esponenziale nel 2025.[30]
Allo stesso modo, un attacco DDoS contro un sito e-commerce può renderlo inaccessibile ai clienti, causando disservizi immediati e perdite di incassi.
Un caso eclatante è stato il malware NotPetya del 2017, che colpì varie multinazionali causando blocchi operativi prolungati: la divisione logistica TNT Express (ovvero FedEx) dovette operare per settimane con sistemi fuori uso, ricorrendo a procedure manuali, e subì danni permanenti su alcuni dati. [31] Al tempo stesso, l'armatore danese Maersk subì, sempre dal NotPetya, la paralisi dei terminal portuali e dei sistemi di spedizione globali. Come conseguenza, l'azienda dovette reinstallare da zero circa 4.000 server e 45.000 computer in dieci giorni, operando manualmente in quasi tutte le attività. Il danno operativo diretto per l'azienda fu stimato intorno ai 300 milioni di dollari e, in aggiunta, Maersk fu costretta a chiudere 76 porti nel mondo, colpendo indirettamente anche la controllata FedEx. [32]

Questi esempi illustrano come un incidente cyber possa tradursi in un fermo operativo, e come l'azienda possa ritrovarsi impossibilitata a erogare servizi e produrre beni per un certo periodo, causando una perdita diretta di ricavi e funzionalità aziendali.

### 1.4.3 Impatto legale e regolamentare

Oltre agli impatti economici e operativi, un grave incidente informatico può esporre l'azienda a conseguenze legali e regolamentari significative. Il primo luogo vi è il tema della compliance normativa: in Europa, durante un attacco in cui vengono sottratti dati personali di clienti o dipendenti interviene il GDPR. Quest'ultimo impone l'obbligo di notifica della violazione al Garante Privacy entro 72 ore dall'attacco, e prevede sanzioni amministrative molto pesanti in caso di inadempienza o carenza nelle misure di

[30] Snape, G. (2025, February 19). Supply chain cyber attacks surge over 400%, expected to continue rising – Cowbell report. *Insurance Business*. https://www.insurancebusinessmag.com/us/news/cyber/supply-chain-cyber-attacks-surge-over-400-expected-to-continue-rising--cowbell-report-525369.aspx
[31] Heller, M. (2017, August 4). ***Ransomware recovery goes beyond data loss for enterprises***. TechTarget. https://www.techtarget.com/searchsecurity/news/450423993/Ransomware-recovery-goes-beyond-data-loss-for-enterprise
[32] Cimpanu, C. (2018, January 25). *Maersk reinstalled 45,000 PCs and 4,000 servers to recover from NotPetya attack*. Bleeping Computer. https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/

protezione, facendo arrivare le multe fino a 20 milioni di euro oppure il 4% del fatturato annuo mondiale dell'azienda. [33]

Negli ultimi anni, molti colossi sono stati sanzionati per violazioni di dati. Tra questi si ricordano Meta (Facebook) che nel 2023 ricevette una multa di 1,2 miliardi di euro, poi anche Amazon multata di 746 milioni di euro, TikTok con 345 milioni e tante altre, dimostrando che le autorità non esitano a colpire con sanzioni molto elevate. [34]

Di seguito vengono riportate le principali sanzioni inflitte per violazioni del GDPR, evidenziando come le autorità europee applichino multe di importi considerevoli per scoraggiare comportamenti non conformi alla normativa sulla protezione dei dati.

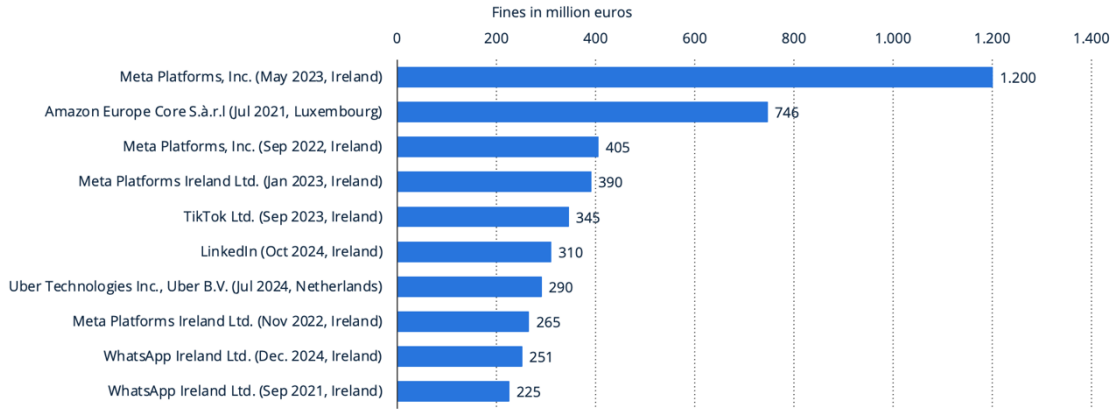



Figura 5: Principali multe per violazioni del GDPR a livello europeo 2021-2025 (milioni di €). Fonte: Statista

A causa dell'aumento degli attacchi informatici e della necessità di maggiore regolamentazione, la direttiva europea NIS del 2016 venne sostituita nel 2023 dalla direttiva NIS2. Quest'ultima istituisce un quadro giuridico unificato per sostenere la cybersicurezza in 18 settori critici in tutta l'UE. Dunque, impone agli Stati membri di rafforzare le loro capacità di materia di sicurezza informatica, introducendo misure di gestione dei rischi ed obblighi di segnalazione ai soggetti di un numero maggiore di settori

[33] European Commission. (n.d.). *What if my company/organisation fails to comply with the data protection rules?* https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-companyorganisation-fails-comply-data-protection-rules_en

[34] Skillcast. (2025, April 22). *20 biggest GDPR fines 2018–2024: Breaches of GDPR*. Skillcast Blog. https://www.skillcast.com/blog/20-biggest-gdpr-fines

e stabilendo norme per la cooperazione, la condivisione delle informazioni, la vigilanza e l'applicazione delle misure di cybersicurezza. [35]

Oltre alle multe dei regolatori, un'organizzazione colpita potrebbe affrontare cause legali civili da parte di clienti, partner commerciali o investitori. Se il *breach* ha causato danni a terzi o ha violato obblighi contrattuali, questi soggetti possono richiedere risarcimenti in sede giudiziaria. Casi rilevanti sono i "*mega-breach*" di Yahoo! e Equifax, a seguito dei quali, entrambe le aziende hanno dovuto affrontare risarcimenti molto onerosi per ripagare i clienti coinvolti. [36]

In settori altamente regolamentati, come quello bancario, assicurativo, sanitario ed energetico, un incidente di sicurezza può inoltre innescare azioni da parte degli enti di vigilanza. Per esempio, nel settore bancario, le autorità di settore come Banca d'Italia, IVASS e organismi europei, possono richiedere ispezioni straordinarie, imporre verifiche di sicurezza indipendenti o ordinare misure correttive immediate. Questo aggiunge un ulteriore livello di pressione normativa sulle organizzazioni colpite da cyber attacchi, specialmente se forniscono servizi critici al pubblico.

Infine, un altro fattore da considerare, è la perdita della proprietà intellettuale. Se gli hacker rubano segreti industriali, algoritmi, formule o codici segreti, l'azienda vede compromesso il proprio vantaggio competitivo e ciò per cui ha lavorato e speso risorse. Oltre al danno economico diretto, vi è una complessa tutela legale, in quanto diventa difficile impedire che le informazioni non finiscano in mano dei competitor o peggio.

### 1.4.4 Impatto reputazionale

L'impatto reputazionale di un cyber attacco è spesso il più subdolo e a lungo termine. Una violazione grave mina la fiducia dei clienti, partner e investitori verso l'azienda colpita, intaccando il capitale reputazionale costruito negli anni. La perdita o sottrazione di dati

[35] European Commission. (s.d.). *Direttiva NIS2: messa in sicurezza delle reti e dei sistemi informativi*. Plasmare il futuro digitale dell'Europa. https://digital-strategy.ec.europa.eu/it/policies/nis2-directive
[36] Sjouwerman, S. (2019, September 28). *Scam of the Week: Yahoo Massive Data Breach Settlement phishing attacks*. KnowBe4. https://blog.knowbe4.com/scam-of-the-week-yahoo-massive-data-breach-settlement-phishing-attacks

sensibili genera un forte senso di tradimento nei consumatori, compromettendo la loro fiducia nei confronti dell'azienda e spingendoli a rivolgersi a concorrenti per prodotti e servizi alternativi.
Studi e sondaggi confermano quanto detto: dopo un cyber attacco significativo, le aziende sperimentano spesso un calo duraturo nel numero di clienti o utenti attivi e un crollo degli indici di fiducia del brand. Secondo un'indagine IDC, l'80% dei consumatori nei paesi sviluppati dichiara che smetterebbe di fare affari con un'azienda dopo una violazione dei suoi dati. In aggiunta, un'analisi del Cloud Security Alliance stima che un'organizzazione vittima di un *breach* possa perdere fino a un terzo della propria base clienti a causa dell'evento, e che la cattiva pubblicità rende poi difficile riconquistarne dei nuovi. [37] Questo "effetto fiducia" negativo di cui si parla, rappresenta spesso la parte più consistente del danno economico. Infatti, sempre secondo l'analisi menzionata prima, nei costi medi di un *breach*, circa il 38% è dovuto alle perdite di business e di clienti.

Altri stakeholder che possono essere coinvolti sono gli investitori. Quando una società quotata divulga una violazione di dati, tipicamente il titolo in Borsa subisce gravi riabbassamenti del prezzo delle azioni e conseguente perdita di capitalizzazione. Un esempio di un'azienda già citata riguarda Equifax. Si tratta di un'agenzia di credito statunitense che nel 2017 subì un furto di 143 milioni di dati dei cittadini, dovendo affrontare conseguenze catastrofiche, tra cui il crollo del valore del titolo in Borsa del 30% e un danno reputazionale duraturo.

Bisogna però specificare che l'entità del danno reputazionale può variare molto in base al settore e a come l'azienda gestisce la crisi. I consumatori non sempre abbandonano in massa il fornitore violato, specialmente se percepiscono trasparenza e impegno nel rimediare. In alcuni casi, aziende violate sono riuscite a riconquistare la fiducia tramite investimenti in sicurezza e campagne di comunicazione efficaci. Tuttavia, settori come quello sanitario, finanziario e tecnologico, in cui la fiducia, oltre ad essere al centro del rapporto, è anche personale, risultano particolarmente vulnerabili sul fronte reputazionale.

[37] Cloud Security Alliance. (2022, September 27). *The ripple effect of a data breach*. https://cloudsecurityalliance.org/blog/2022/09/27/the-ripple-effect-of-a-data-breach

Questi aspetti verranno approfonditi meglio nei successivi capitoli.

## 1.5 L'importanza strategica della cybersecurity per le aziende: risk management e governance

Dopo aver analizzato le principali caratteristiche e i fondamenti della cybersicurezza, è ora possibile comprendere come questa disciplina si sia evoluta nel tempo, passando da un tema prevalentemente tecnico ad una priorità strategica per le aziende di ogni settore. Diversi fattori hanno contribuito a questa trasformazione. Innanzitutto, gli attacchi informatici sono divenuti tra i principali rischi globali per impatto e probabilità, al pari dei cambiamenti climatici e delle crisi geopolitiche. Come sottolineato prima, le minacce cyber sono cresciute in frequenza e sofisticazione, con costi di violazioni in continuo aumento. Parallelamente, è cresciuta la pressione normativa, specialmente in Europa e negli Stati Uniti, per migliorare la resilienza cyber, così come le aspettative dei clienti e degli investitori sulla protezione dei dati e la continuità del business. In sintesi, oggi è ampiamente riconosciuto che la resilienza informatica è parte integrante della resilienza aziendale. Pertanto, un'impresa non può considerarsi ben gestita se non sa proteggere i propri asset digitali e reagire efficacemente agli incidenti cyber. [38]

Di conseguenza, la sicurezza informatica è entrata a pieno titolo nel risk management aziendale e nella corporate governance. I Consigli di Amministrazione e il top management sono chiamati a occuparsi attivamente di cyber risk al pari dei rischi finanziari, operativi e reputazionali. Il World Economic Forum afferma chiaramente che il rischio cyber e tecnologico *"deve essere governato in qualunque organizzazione moderna"*. [39] Per fare ciò, i leader aziendali hanno bisogno di comprendere i temi chiave della cybersecurity e definire strategie di cyber resilienza allineate agli obiettivi di business, per far sì che le questioni di sicurezza informatica non impattino direttamente la fiducia degli stakeholder e dei clienti, e la reputazione dell'organizzazione stessa.

[38] **World Economic Forum. (2024).** *Global cybersecurity outlook 2024: Fortifying the future*. World Economic Forum.
[39] World Economic Forum. (n.d.). *Cyber risk and corporate governance*. https://www.weforum.org/projects/cyber-risk-leadership-and-corporate-governance/

Per dimostrare quanto detto, molti studi evidenziano che i CdA partecipano attivamente, fissando obiettivi chiari, assegnando risorse adeguate e monitorando la preparazione agli incidenti, migliorando le difese delle aziende. Un'indagine globale ha rilevato che una maggiore attenzione del consiglio di amministrazione porta a un incremento medio del 24% del budget per la sicurezza e a una migliore identificazione dei rischi chiave, consolidando una cultura di sicurezza e allineando la gestione cyber con gli obiettivi di business. [40]

Dunque, un efficace governo del rischio cyber "apre le linee di comunicazione tra dirigenti e direttori, trattando la cybersecurity come una questione economica" e non meramente tecnologica.

### 1.5.1 Cybersecurity e risk management

Da un punto di vista di risk management, la cybersecurity viene ormai trattata con gli strumenti tipici della gestione dei rischi aziendali, seguendo l'approccio Enterprise Risk Management (ERM), come il framework COSO (*Committee of Sponsoring Organizations)*. Quest'ultimo ha definito regole, procedure e principi, affinché le organizzazioni possano progettare e valutare i controlli interni, garantire l'integrità, prevenire le frodi e allineare i proprio obiettivi, anche nell'ambito informatico. [41]

A seguito della necessità, da parte delle organizzazioni, di maturare il proprio approccio alla cybersicurezza, la figura del Chief Information Security Officer (CISO) è diventata centrale nel panorama aziendale moderno. [42] Il CISO svolge il ruolo di consulente strategico, responsabile non solo della supervisione delle operazioni legate alla sicurezza delle informazioni, ma anche della definizione di politiche, procedure e strategie dell'organizzazione in materia di protezione dei dati. Le sue mansioni comprendono l'identificazione, l'analisi e la gestione dei rischi, l'implementazione di strumenti e tecnologie adeguate, la supervisione delle conformità alle normative e agli standard di sicurezza, ed infine, la conduzione delle attività di risposta agli incidenti.

---

[40] Internet Security Alliance, & Organization of American States. (n.d.). *Cyber-risk oversight handbook for corporate boards*.

[41] Chowdhury, M. R. (2024). *Analyzing COSO Framework, Objectives, and Implementation* (Week 6 Research Paper, Purdue University Global).

[42] Ramezan, C. A. (2024). *The evolving role of the Chief Information Security Officer (CISO) in modern cybersecurity governance* (Doctoral dissertation, Purdue University). ProQuest Dissertations Publishing.

Dunque, questo ruolo rappresenta un ponte fondamentale tra il reparto IT e la direzione aziendale, trasmettendo informazioni essenziali sui rischi e sulle necessità di investimento nel campo della sicurezza informatica. [43] In aggiunta, per poter svolgere efficacemente il loro compito, i CISO devono adottare un approccio integrato lavorando a stretto contatto con altre funzioni (ad esempio quella legale, compliance o *operations*) garantendo che la strategia di cybersecurity non solo rispetti le norme in evoluzione, ma supporti gli obiettivi dell'azienda.

Questo approccio integrato è fondamentale per passare da un orientamento reattivo a uno proattivo. Incorporare i rischi informatici nell'ERM consente di anticipare le minacce, stimare l'impatto potenziale di eventi cyber sul business, predisporre controlli preventivi e piani di continuità operativa, assicurando la conformità normativa. [44]

### 1.5.2 Impatto normativo e ruolo della corporate governance

Un altro elemento della valenza strategica è il collegamento con la corporate governance e la fiducia degli investitori. Gli investitori istituzionali e i mercati prestano crescente attenzione alla sicurezza informatica tramite società di rating e indici ESG che includono metriche di cyber resilienza nelle loro valutazioni e, di conseguenza, eventuali fallimenti clamorosi in quell'ambito possono portare all'abbassamento del giudizio di affidabilità di un'azienda. [45] Come affermato anche nel paragrafo precedente, le linee guida di una buona governance raccomandano ai consigli di trattare la cybersecurity come una funzione strategica continuativa e discutere regolarmente dello stato della sicurezza, delle risorse allocate e della preparazione ai possibili incidenti. Un esempio, sono le linee guida della National Association of Corporate Directors (NACD) e la Internet Security Alliance (ISA), i cui parametri mirano a creare una solida corporata governance per mantenere stabile l'economia, creare valore aziendale in modo sostenibile. In pratica, come già reso noto, la cybersecurity è diventata un tema da trattare a livello di governo aziendale, con policy, ruoli e responsabilità chiare, con anche il costante monitoraggio di KPI di

[43] Ciekanowski, M., Żurawski, S., Ciekanowski, Z., Pauliuchuk, Y., & Czech, A. (2024). *Chief Information Security Officer: A vital component of organizational information security management*. European Research Studies Journal, 27(2), 35–46.
[44] Siddiqui, J., & Sultana, N. (2023). Exploring enterprise risk management practices: Evidence from an emerging economy. *Journal of Accounting & Organizational Change*, **19**(2), 328–353.
[45] World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*. World Economic Forum

sicurezza e integrazione nelle decisioni aziendali strategiche. In sostanza, tutte le movimentazioni e progetti aziendali devono tener conto dei rischi cyber associati. [46]

### 1.5.3 Cybersecurity come leva strategica e vantaggio competitivo

Invece, per quanto riguarda il punto di vista strategico-competitivo, va considerato che un'efficace strategia di cybersecurity può diventare un vantaggio competitivo per le aziende. In mercati come quello bancario, assicurativo, del commercio elettronico, i clienti scelgono sempre più fornitori affidabili anche sul fronte della protezione dei loro dati. Del resto, un'azienda che dimostra trasparenza e solidità nella gestione della sicurezza può guadagnare la fiducia del mercato e distinguersi dai concorrenti meno diligenti. Al contrario, subire incidenti frequenti o gravi, mina la reputazione e può far perdere quote di mercato.

Ma come fa un'azienda a dimostrare di gestire la sicurezza in modo sicuro ed ottimale? Ad oggi, esistono certificazioni che si basano sulle linee guida del NIST e che aderiscono a specifici schemi di certificazione settoriali. Tra queste vi è la certificazione ISO/IEC 27001, ovvero uno standard internazionale che definisce i requisiti per la gestione della sicurezza informatica, ed aiuta tutte le aziende in tutti i settori a identificare e mitigare le vulnerabilità. [47] Difatti, ottenere questa certificazione è un segnale concreto di affidabilità, e significa che l'azienda aderisce alle migliori pratiche globali di sicurezza e ha sottoposta a verifica l'efficacia del proprio sistema di controllo.

Un'ulteriore dimensione strategica della cybersecurity risiede nella collaborazione intersettoriale e pubblico-privata. Le minacce informatiche odierne sono così pervasive e complesse che nessuna organizzazione può fronteggiarle da sola. Perciò, si sta affermando sempre di più una visione "ecosistemica" della sicurezza: aziende di vari settori, uniscono le informazioni in reti condivise e collaborano attivamente con le autorità. Più nel dettaglio, un esempio sono gli ISAC (Information Sharing and Analysis Centers) che forniscono un meccanismo centralizzato per raccogliere e condividere informazioni su minacce, vulnerabilità e incidenti tra organizzazioni in uno stesso settore

[46] World Economic Forum. (n.d.). *Cyber Risk Leadership and Corporate Governance*.
[47] International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements*.

o settori diversi. Questo approccio permette ai diretti interessati di prepararsi a reagire in modo coordinato alle nuove minacce,[48] dimostrando sempre di più quanto le nuove sfide cyber riguardino il mondo intero, e soprattutto, può fungere come ponte tra il settore privato e le autorità pubbliche, contribuendo ad una strategia difensiva coordinata a livello di "sistema-paese".
Altre piattaforme simili che hanno lo scopo di condividere informazioni critiche e sviluppare capacità comuni di risposta sono *l'European Cybersecurity Organisation* in Europa, e la CISA (*Cybersecurity and Infrastructure Security Agency*) negli USA.

Dunque, la sicurezza informatica oggi è una priorità riconosciuta ai massimi livelli aziendali. I vertici organizzativi hanno la responsabilità di assicurare che la strategia di cybersecurity sia allineata con quella di business, al fine di garantire la continuità operativa e promuovere la resilienza digitale come elemento centrale della governance aziendale.

## 1.6 Tendenze emergenti: AI, IoT, "Crime-as-a-Service", supply chain e minacce geopolitiche

Come illustrato nei paragrafi precedenti, il mondo cyber è in costante mutamento e alcune tendenze emergenti stanno ridefinendo il panorama delle minacce informatiche e delle modalità di difesa. Tra queste si possono individuare l'Intelligenza Artificiale, l'Internet of Things (Internet delle cose), il Crime-as-a-Service, attacchi informatici alle supply chain e le minacce geopolitiche. Queste tendenze contribuiscono ad aumentare la complessità e la pericolosità degli attacchi, richiedendo contromisure sempre più sofisticate. Secondo il Global Security Outlook 2025, i principali fattori che contribuiscono alla complessità della cybersecurity sono i seguenti:

[48] Lange, K. (2023, ottobre 18). *ISACs: Information Sharing & Analysis Centers*. Splunk. https://www.splunk.com/en_us/blog/learn/isacs-information-sharing-analysis-centers.html

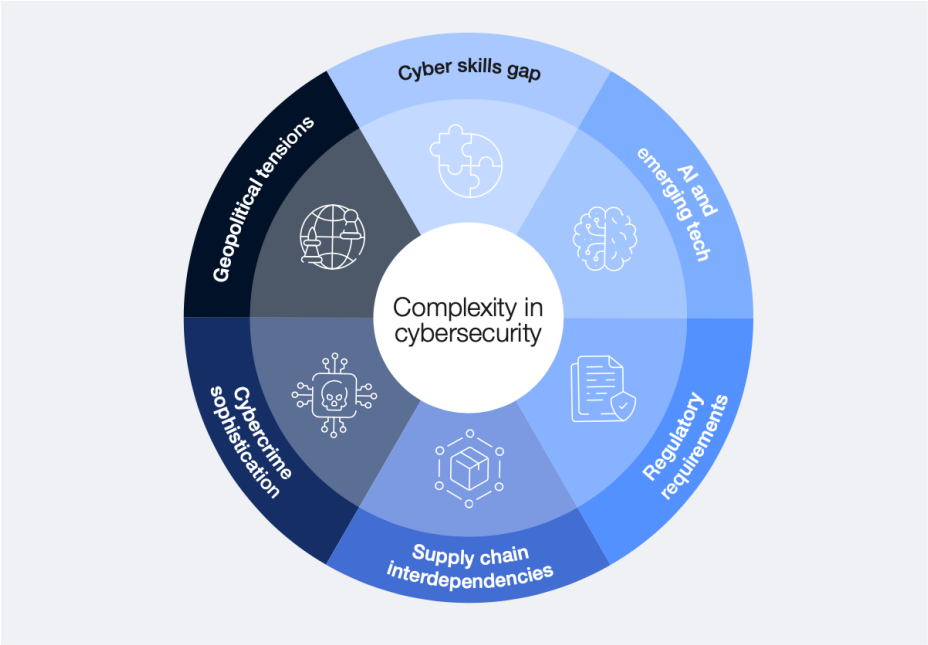



Figura 6: Principali driver della complessità nella cybersecurity a livello globale. Fonte: World Economic Forum

La Figura 6 illustra come la complessità della cybersecurity non dipenda da un solo aspetto, ma da una serie di fattori che si intrecciano tra loro. Ad esempio, le tensioni geopolitiche, stanno trasformando gli attacchi informatici in veri e propri strumenti di pressione politica, mentre la criminalità informatica diventa ogni giorno più organizzata e difficile da contrastare. A complicare ulteriormente lo scenario c'è la forte interdipendenza delle catene di fornitura, facendo in modo che una sola falla in un fornitore possa mettere a rischio l'intero sistema. Anche le normative in continua evoluzione richiedono alle aziende sforzi costanti di adattamento, aumentando la complessità gestionale. In aggiunta, l'arrivo di nuove tecnologie, e in particolare dell'intelligenza artificiale, apre enormi opportunità, ma allo stesso tempo introduce nuove vulnerabilità che ancora non sono pienamente gestibili. Infine, la carenza di professionisti qualificati nel settore rende ancora più difficile far fronte a queste sfide.

Questi fattori verranno analizzati e approfonditi nei seguenti paragrafi.

### 1.6.1 Intelligenza artificiale e machine learning

Come è già stato accennato, l'IA e il machine learning rappresentano un paradosso, ovvero hanno un impatto ambivalente sulla cybersecurity. Da una parte sono sempre più

diffusi strumenti di difesa basati su queste due nuove tecnologie che hanno l'obiettivo di rilevare minacce, analizzando una grande mole di dati in tempo reale, identificando anomalie, utilizzando algoritmi che imparano a riconoscere comportamenti malevoli e riescono a generare risposte immediate per contrastare il problema.[49] Dall'altro lato, i criminali informatici stanno iniziando a sfruttare l'intelligenza artificiale per potenziare i propri attacchi.[50]

Gli attacchi che utilizzano l'IA si possono dividere in due categorie principali:

- Attacchi assistiti dall'Intelligenza Artificiale, in cui le tecnologie di IA e machine learning vengono impiegate per aiutare gli hacker umani a pianificare o eseguire attacchi informatici;
- Attacchi autonomi condotti da IA, in cui agenti dotati di intelligenza artificiale e machine learning effettuano attacchi informatici in modo autonomo, senza intervento umano, colpendo diversi settori industriali.

Tra le minacce generate dall'utilizzo di IA emergono:

- *Deepfake*: attacchi basati su contenuti multimediali falsi ma realistici, come immagini, video, audio, testi, creati tramite IA e ML per ingannare o impersonificare persone o sistemi, aumentando l'efficacia del social engineering. Possono dunque essere utilizzati per diffondere disinformazione, ricattare, simulare autenticazioni biometriche e altro ancora. Spesso, questi contenuti vengono creati per ingannare i sistemi di cybersicurezza, risultando capaci di sfuggire ai sistemi di controllo.
- *Botnet*: si tratta di una rete di dispositivi interconnessi controllati da criminali informatici per eseguire vari tipi di attacchi. Di solito, possono essere impiegate per attacchi DDoS, spam, furto di dati e altro. Anche in questo caso, l'uso di IA e ML permette di identificare vulnerabilità, automatizzare gli attacchi, aumentare la velocità e coordinare le azioni, rendendo il rilevamento più difficile.
- *Reinforcement Learning* (Apprendimento per rinforzo): questa tecnica consente agli agenti autonomi dotati di IA di apprendere dalle proprie esperienze, adattarsi,

[49] Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2023). *Cyber security: State of the art, challenges and future directions*. Cyber Security and Applications, 2, 100031.
[50] Heiding, F. (2025, May 13). *72% of cyber leaders say risks are rising. Here's how states and businesses are responding*. World Economic Forum.

ottimizzare le strategie di attacco e automatizzare i processi di sfruttamento delle vulnerabilità sulla base delle risposte ricevute dal sistema bersaglio. [51]

Si può notare come gli attacchi informatici basati sull'Intelligenza Artificiale rappresentino una forma di minaccia più complessa e sofisticata, tanto da divenire una delle principali preoccupazioni delle organizzazioni in termini di sicurezza. [52] L'ENISA, nel Threat Landscape del 2024, ha evidenziato come i criminali stiano già migliorando i risultati delle campagne di *phishing* grazie all'IA e sviluppando *malware* più abili nell'evitare i sistemi di difesa. Inoltre, l'uso di strumenti di *generative AI* sta contribuendo ad aumentare il numero e la precisione degli attacchi di social engineering, con mail di *phishing* più credibili e personalizzate, e audio/video falsi difficilmente distinguibili dal vero. In aggiunta a ciò, un recente rapporto Europol segnala come gli hacker stiano già sfruttando i modelli generativi per creare truffe perfette che coincidono con il profilo della vittima in modo preciso. [53]
Di conseguenza, sta emergendo una sorta di "corsa agli armamenti" in cui l'IA utilizzata in modo dannoso e l'IA difensiva si scontrano, ed inoltre, le difese tradizionali risultano poco utili, rendendo necessaria un'evoluzione dei sistemi di sicurezza.

Di fatto, il grafico sottostante dimostra e conferma quanto detto in questo paragrafo. L'emergere dell'intelligenza artificiale generativa (47%) rappresenta il driver più influente delle azioni di cybersecurity, riflettendo la consapevolezza di tali tecnologie, che pur offrendo notevoli opportunità di automazione, analisi avanzata e ottimizzazione dei processi, introducono al contempo nuove superfici di attacco e modalità di minaccia.

[51] Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2023). *Cyber security: State of the art, challenges and future directions*. Cyber Security and Applications, 2, 100031.
[52] World Economic Forum. (2025, 13 gennaio). *Global Cybersecurity Outlook 2025*.
[53] Directorate-General for Migration and Home Affairs. (2025, 16 giugno). *Europol published report on how cybercriminals trade and exploit data*. European Commission. https://home-affairs.ec.europa.eu/news/europol-published-report-how-cybercriminals-trade-and-exploit-data-2025-06-16_en

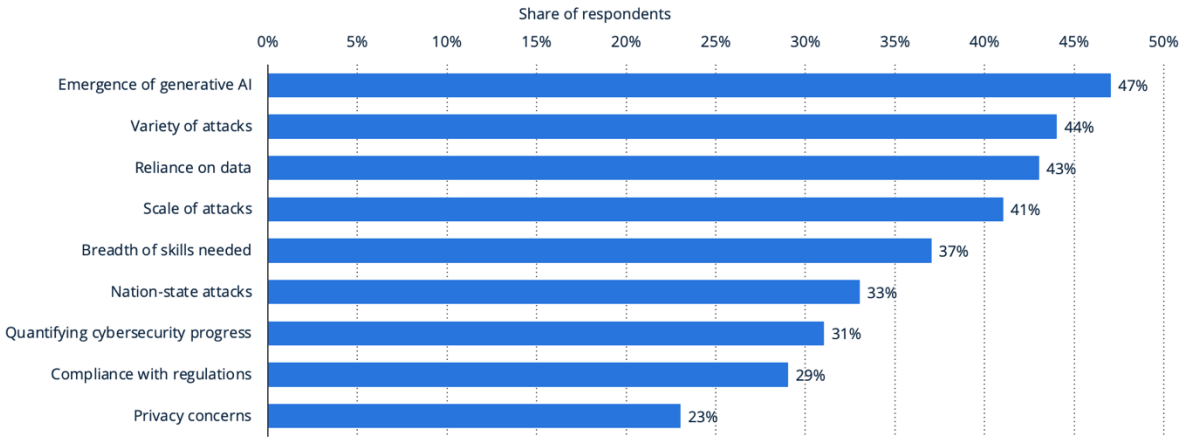



Figura 7: Fattori chiave che influenzano le strategie di cybersicurezza a livello globale nel 2024. Fonte: Statista

### 1.6.2 Internet of Things (IoT)

La rapida proliferazione dell'Internet of Things (IoT) ha rivoluzionato le industrie, ridefinito le esperienze dei consumatori e trasformato l'economia digitale. Dai dispositivi domestici e ai monitor sanitari, ai sistemi di controllo industriale e ai veicoli connessi, i dispositivi IoT sono diventati parte integrante della vita moderna.

Pertanto, negli ultimi dieci anni, il settore dell'IoT ha registrato una crescita costante e si prevede che tale tendenza proseguirà ulteriormente, fino a raggiungere un valore stimato di 1.559,89 miliardi di dollari entro il 2029.

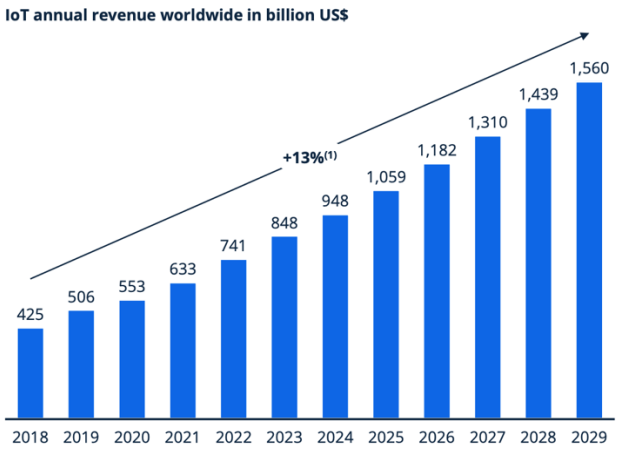



Figura 8: Andamento dei ricavi annuali globali dell'IoT, 2018-2029 (mld US$). Fonte: Statista

Questa crescita esponenziale genera volumi di dati senza precedenti, una moltitudine di endpoint in rete e una vasta superficie d'attacco pronta per essere sfruttata. [54] Sebbene, l'IoT apre nuove strade per l'efficienza, l'automazione e l'analisi in tempo reale, comporta anche una serie di preoccupazioni in merito alla privacy dei dati, alla sicurezza delle reti, alla resilienza operativa e all'aumento di attacchi informatici.

A differenza dei sistemi IT tradizionali, gli ecosistemi IoT presentano vincoli e vulnerabilità uniche che richiedono approcci di sicurezza specializzati. Tra queste criticità rientrano le risorse limitate e le capacità di calcolo e memoria ridotte dei dispositivi, che rendono difficile l'implementazione dei sistemi di sicurezza. Di conseguenza, gli aggiornamenti sono rari e non possono avvenire da remoto, rendendo complicato ed impossibile correggere le vulnerabilità. Infine, l'assenza di standard comuni e di uniformità in questo contesto rende ancora più difficile rilevare le minacce e proteggere i dati trasmessi. Per questa serie di problematiche e lacune, i dispositivi IoT sono sempre più nel mirino e se non vengono adeguatamente protetti, possono essere utilizzati per rubare dati, spiare utenti e interrompere servizi. [55]

Le tendenze attuali evidenziano dunque la necessità di rafforzare la sicurezza dell'IoT, puntando su standard e certificazioni specifiche per i dispositivi, sull'adozione di soluzioni di segmentazione di rete per isolare i dispositivi meno sicuri, sull'implementazione di meccanismi di autenticazione robusti e sull'utilizzo di tecnologie come la blockchain per garantire l'integrità delle comunicazioni tra macchine. [56]

Il grafico sottostante dimostra una crescita significativa del mercato globale della sicurezza nell'Internet of Things, passando da 5 miliardi di dollari nel 2022 a 31 miliardi nel 2027. Tale incremento, rispecchia ciò che è stato affermato precedentemente, ovvero l'aumento della domanda di soluzioni di protezione per dispostivi connessi, determinando

[54] Avnet Staff. (2024, 15 marzo). *Solving the three major IoT challenges: Power supply, software fragmentation, and deployment*. Avnet. https://www.avnet.com/apac/resources/article/solving-the-three-major-iot-challenges/
[55] Balroop, D. (2025, May 15). *Cybersecurity and IoT: Securing billions of connected devices*. LinkedIn.
[56] Blue Goat Cyber. (2024, novembre 17). *Top IoT cybersecurity trends to watch in 2025*.

sia l'espansione dell'IoT in diversi settori ed anche l'esigenza di mitigare i crescenti rischi informatici.

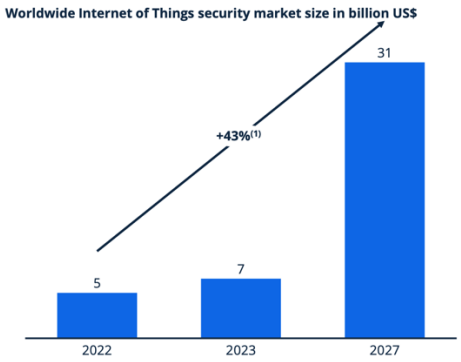



Figura 9: Crescita del mercato mondiale della sicurezza per l'IoT 2022-2027 (mld US$). Fonte: Statista

### 1.6.3 Crime-as-a-Service

Parallelamente all'evoluzione delle minacce, si è consolidato un vero e proprio mercato nero dei servizi cybercriminali, il cosiddetto Crime-as-a-Service (CaaS). In questo contesto, le competenze e gli strumenti necessari per condurre attacchi informatici vengono commercializzati al migliore offerente, abbassando drasticamente la barriera d'ingresso per chi intende delinquere online.

Secondo l'Internet Organised Crime Threat Assesment di Europol, oggi i cybercriminali non hanno più bisogno di competenze tecniche avanzate per avere successo, perché esistono piattaforme CaaS che offrono di tutto, dai database di dati rubati a tutorial dettagliati per frodi, fino a "pacchetti" chiavi in mano per condurre campagne di phishing o ransomware. Sui forum è possibile acquistare accessi a sistemi compromessi, noleggiare infrastrutture di comando e controllo, oppure ottenere supporto su misura. Il Ransomware-as-a-Service (RaaS), in particolare, ha avuto un ruolo chiave nell'esplosione del fenomeno ransomware degli ultimi anni, portando gruppi di criminali sofisticati a sviluppare il malware e gestire l'infrastruttura, mentre una miriade di affiliati meno esperti effettua materialmente le intrusioni e la distribuzione del ransomware, spartendo poi i proventi del riscatto con gli sviluppatori. Questo modello di "franchising" ha reso il ransomware pervasivo, perché anche criminali di medio-basso livello possono lanciare attacchi devastanti semplicemente aderendo a un programma RaaS.

Gli effetti del CaaS sono di vasta portata, e sono legati alla proliferazione di attacchi su scala globale, alla sofisticazione crescente e grande reattività nell'utilizzare nuove vulnerabilità, "democratizzando" il crimine informatico e creando un'economia sommersa estremamente redditizia e resiliente.

### 1.6.4 Supply chain

Dopo il clamoroso caso SolarWinds nel 2020, gli attacchi informatici alla catena di fornitura digitale sono emersi come una delle tendenze più pericolose a livello globale. Invece di colpire direttamente un bersaglio finale ben protetto, l'attaccante compromette un fornitore di software o servizi fidato, inserendo malware in componenti che verranno poi distribuite a cascata a molte organizzazioni. Il risultato è un'infezione su larga scala, difficile da rilevare perché proveniente da componenti legittime. Secondo ENISA, gli attacchi alle supply chain rientrano oggi tra le prime minacce nel panorama cyber. [57]

A conferma di ciò, il seguente chart dimostra le principali sfide della cybersecurity registrate nel 2024. Prima tra queste è proprio la vulnerabilità nelle interdipendenze nelle supply chain, indicata dal 26% dei rispondenti come la sfida principale da affrontare per garantire la sicurezza informatica aziendale.

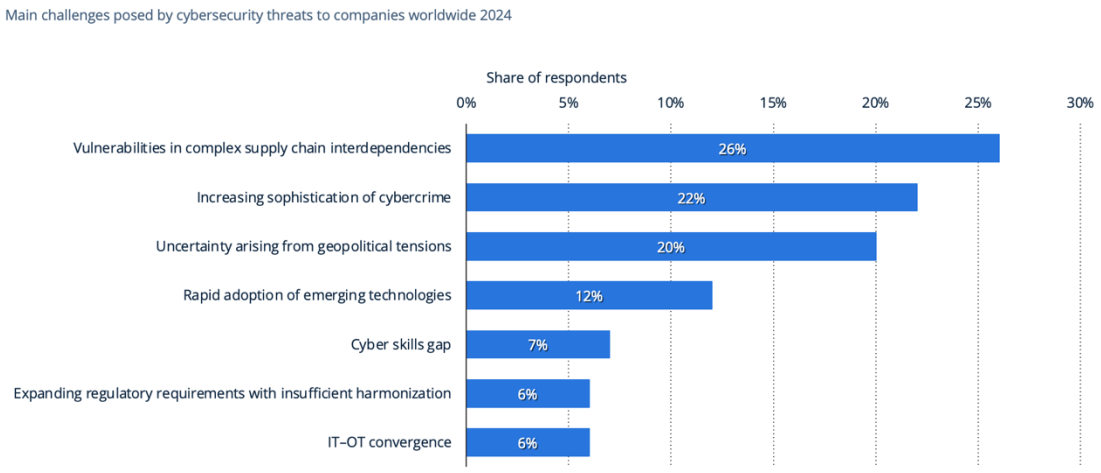



Figura 10: Le principali minacce di cybersecurity percepite dalle imprese nel mondo (2024). Fonte: Statista

[57] European Union Agency for Cybersecurity. (2024, September). *ENISA threat landscape 2024: July 2023 to June 2024*. Publications Office of the European Union. https://doi.org/10.2824/0710888

Questo riflette un fatto che si sta sviluppando sempre di più in questi ultimi anni, ovvero che le aziende dipendono per lo più da fornitori di software esterni, servizi cloud, librerie open source ecc., facilitando agli hacker lo sfruttamento di anelli deboli per colpire indirettamente bersagli altrimenti ben protetti.

Riprendendo l'esempio citato all'inizio, SolarWinds è spesso utilizzata dai governi per monitorare le attività network e i sistemi federali. Pertanto, l'incidente ha permesso di infettare fino a 18.000 aziende ed enti governativi attraverso un aggiornamento software manomesso. [58] Analogamente, nel 2021 l'attacco a Kaseya (software di gestione IT) ha distribuito ransomware a centinaia di aziende MSP (Managed Service Provider) o loro clienti. Attraverso la compromissione di un singolo aggiornamento del software, gli aggressori sono riusciti a colpire indirettamente tra 800 e 1.500 aziende nel mondo.
Questi attacchi sono considerati "game-changer", in quanto amplificano enormemente l'impatto: colpendo un solo punto (il fornitore), l'hacker utilizza un moltiplicatore che dà l'accesso a molte vittime in contemporanea. Inoltre, spesso si tratta di attacchi sofisticati e sponsorizzati da attori statali, infatti, come è noto, nel caso SolarWinds, l'operazione è stato attribuita ad un'unità di intelligence russa (APT) con finalità di spionaggio di alto profilo. [59]

Pertanto, la tendenza odierna è verso un approccio "supply chain security" più rigoroso: le aziende sono incoraggiate a valutare i rischi cyber dei propri fornitori e partner, a pretendere livelli di sicurezza adeguati contrattualmente e a implementare controlli come l'analisi dei software per tracciare componenti di esso provenienti da terze parti. Contestualmente, normative come NIS2 richiedono esplicitamente agli Stati membri dell'UE di valutare le vulnerabilità dei propri fornitori e prestatori di servizi, segnalando tempestivamente eventuali incidenti significativi alle autorità competenti. [60]
In sostanza, la sicurezza non è più confinata all'interno dei muri dell'azienda, ma deve abbracciare l'intero ecosistema di fornitori e partner.

[58] U.S. Government Accountability Office. (2021, 22 aprile). *SolarWinds cyberattack demands significant federal and private-sector response (infographic)*.
[59] U.S. Government Accountability Office. (2021, 22 aprile). *SolarWinds cyberattack demands significant federal and private-sector response (infographic)*.
[60] Laitila, A., & Mikkola, K. (2024, gennaio). *Understanding NIS2: The New EU Cybersecurity Directive*. Deloitte Finland.

### 1.6.5 Minacce geopolitiche e cyber warfare

Negli ultimi anni, la guerra informatica è diventata una delle principali preoccupazioni per governi, eserciti e aziende strategiche. L'arena cyber si è trasformata in un vero e proprio terreno di scontro tra Stati, utilizzato per perseguire obiettivi geopolitici e strategici. Gli episodi registrati dal 2015 al 2023 dimostrano come gli attacchi digitali non siano solo eventi isolati, ma parte integrante di campagne coordinate e finanziate da nazioni, con obiettivi che vanno dallo spionaggio e dal furto di dati governativi o segreti industriali, fino al sabotaggio di infrastrutture critiche e alle interferenze nei processi democratici, ad esempio tramite attacchi ai sistemi elettorali o la sottrazione di dati sensibili di esponenti politici. [61]

Il legame tra i conflitti geopolitici e le operazioni informatiche appare evidente soprattutto dopo l'invasione dell'Ucraina da parte della Russia. Infatti, la guerra è stata preceduta e accompagnata da una campagna cibernetica su vasta scala, che comprende attacchi alle infrastrutture energetiche e IT, azioni di sabotaggio e operazioni di disinformazione. Il rapporto rilasciato da ENISA sottolinea come la guerra in Ucraina abbia ridisegnato il panorama delle minacce, incrementando l'*hacktivismo* e l'uso degli attacchi informatici come "armi supplementari" nei conflitti.
Parallelamente, il cyber-spionaggio industriale è emerso come un fronte altrettanto critico, in cui alcuni gruppi rubano ingenti somme di criptovalute per finanziare regimi, ed altri si concentrano sul furto di tecnologie avanzate. [62]

Nel Global Cybersecurity Outlook 2025, un CEO su tre cita il cyber-spionaggio e il furto di proprietà intellettuale come due tra le principali preoccupazioni per le aziende. Pertanto, ciò evidenzia come le minacce geopolitiche non riguardano solo i governi, ma anche le aziende che operano in settori strategici, tra cui quelli di difesa, energetici, alta tecnologia e finanza. Di fronte a questo scenario, sta emergendo la necessità di una maggiore collaborazione tra pubblico e privato in materia di difesa nazionale. Come già

[61] European Union Agency for Cybersecurity (ENISA). (2023, ottobre). *ENISA Threat Landscape 2023*.
[62] Heiding, F. (2025, 13 maggio). *72% of cyber leaders say risks are rising. Here's how states and businesses are responding*. World Economic Forum.

menzionato nel paragrafo 1.5.3, molti Stati si sono dotati di strategie nazionali di cybersecurity e centri di risposta che lavorano con aziende private per condividere informazioni su attacchi di matrice statale e preparare piani di resilienza. In più, si discute a livello internazionale di norme di comportamento nel cyberspazio e di accordi per limitare certe attività ostili.

In parallelo ai conflitti tra Stati, la dimensione geopolitica coinvolge anche il cyberterrorismo e l'*hacktivismo*. Il primo riguarda il rischio che gruppi terroristici potrebbero colpire infrastrutture vitali attraverso il cyberspazio, mentre il secondo, è di matrice politica/ideologica. Ad esempio, a seguito della guerra in Ucraina si è osservato un aumento di attacchi DDoS rivendicati da collettivi di attivisti digitali schierati con l'una o l'altra parte, nel tentativo di influenzare l'opinione pubblica o danneggiare il morale nemico.

### 2.6.6 Mancanza di professionisti nell'ambito cyber

Dall'analisi svolta dal Global Security Outlook 2025 emerge che dal 2024 il divario di competenze in ambito cyber è aumentato dell'8%, con due organizzazioni su tre che segnalano lacune, tra cui la mancanza di talenti e competenze essenziali per soddisfare le proprie esigenze di sicurezza. Inoltre, solo il 14% delle imprese si dichiara sicuro di disporre, ad oggi, delle persone e delle competenze necessarie.

Questi numeri dimostrano quanto il gap di competenze rappresenti una delle principali criticità per le organizzazioni, limitandone la capacità di difendersi in modo efficace dalle minacce informatiche e di sviluppare strategie di sicurezza adeguate alle sfide emergenti.

Il grafico sottostante mostra il divario nella forza lavoro della cybersecurity a livello mondiale nel 2024, suddiviso per regione, e rappresenta il numero stimato di professionisti mancanti (in migliaia).

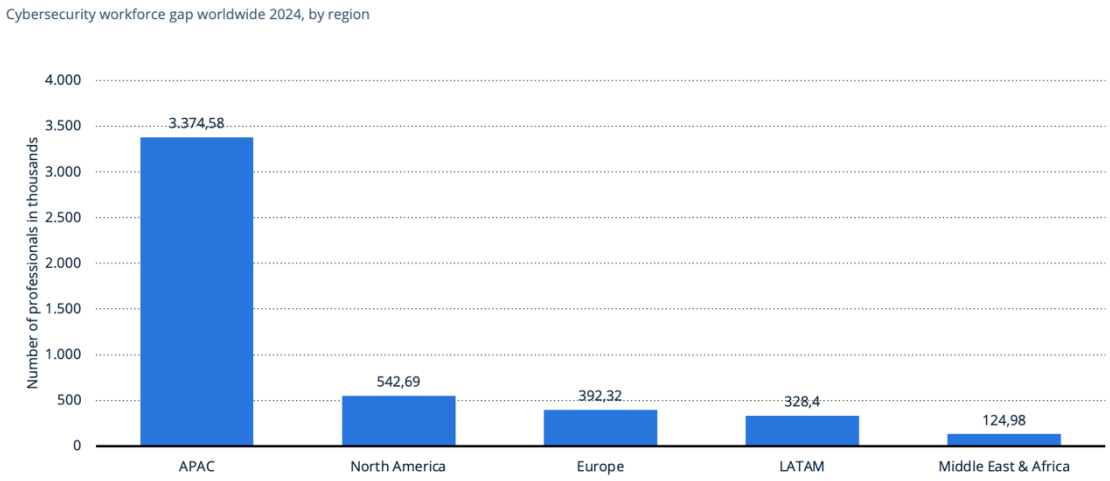



Figura 11: Gap della forza lavoro nella cybersecurity a livello mondiale, per area geografica (2024). Fonte: Statista

Nella Figura 11 si osserva che l'area APAC (Asia-Pacifico) registra il divario più elevato con oltre 3,37 milioni di professionisti mancanti, a seguire il Nord America, l'Europa, l'America Latina e il Medio Oriente con l'Africa. Pertanto, si evince che l'area APAC presenta la più ampia carenza di professionisti in ambito cybersecurity, con conseguenze rilevanti sul modo in cui le organizzazioni sono in grado di affrontare attacchi e criticità.

Dunque, guardando al futuro, il panorama cyber sarà caratterizzato da attacchi sempre più automatizzati e potenziati dall'IA, una superficie di attacco estesa da miliardi di dispositivi interconnessi, un ecosistema criminale che offre *malware* e servizi chiave in mano, minacce subdole nascoste nella filiera digitale e un ruolo crescente di motivazioni geopolitiche dietro molti attacchi. Da ciò ne deriva che la resilienza informatica diventerà sempre più un fattore importante di competitività e di sicurezza nazionale.

### 1.7 Panorama normativo

Il contesto normativo e degli standard in ambito cybersecurity si è notevolmente ampliato nell'ultimo decennio a livello internazionale, fornendo alle organizzazioni un quadro più uniforme di regole e standard di riferimento per elevare il livello di sicurezza informatica e la protezione dei dati. Per avere una visione più chiara ed ampia, si è fatta una

distinzione tra i vari framework presenti in Europa e negli Stati Uniti, dimostrando che i regolamenti utilizzati spesso differiscono, anche se perseguono lo stesso obiettivo.

### 1.7.1 GDPR (General Data Protection Regulation)

Il Regolamento Generale sulla Protezione dei Dati (UE 2016/679), in vigore dal maggio 2018, ha ridefinito il panorama globale della privacy e della sicurezza dei dati. È considerata la normativa sulla privacy e sicurezza più rigorosa al mondo, imponendo obblighi anche a organizzazioni extra-UE purché trattino dati personali di persone nell'Unione Europea, seguendo il principio di extraterritorialità. Il GDPR sancisce che i dati personali appartengono innanzitutto all'individuo, non a chi li gestisce, e richiede alle aziende di adeguare i propri processi per garantire tutela dei diretti interessati. [63]

Entrando più nel dettaglio, il GDPR si fonda su valori come la trasparenza nei confronti degli interessati e la responsabilizzazione di chi tratta i dati, richiedendo robuste misure organizzative di governance per minimizzare il rischio di violazioni. Dunque, in pratica, il Regolamento impone misure concrete, tra cui:

- L'obbligo di mantenere registri interni delle attività di protezione dei dati dimostrando conformità;
- Il requisito di notificare senza ingiustificato ritardo le autorità di vigilanza in caso di violazione dei dati (le organizzazioni devono segnalare i *data breach* entro 72 ore), documentando i fatti, le conseguenze e le azioni correttive intraprese;
- La nomina di un Responsabile della Protezione dei Dati (DPO) obbligatoria per alcune tipologie di organizzazioni.

Tali requisiti di processo mirano a strutturare e formalizzare la gestione dei dati, creando un ambiente in cui la sicurezza e la privacy siano parte integrante delle operazioni aziendali.

Un ulteriore elemento fondamentale da considerare è il severo regime sanzionatorio del GDPR. In caso di non conformità, le autorità di controllo possono emettere avvertimenti, ordinare la sospensione (temporanea o definitiva) dei trattamenti illeciti, e imporre pesanti multe amministrative. Inoltre, le violazioni più gravi possono comportare sanzioni fino a 20 milioni di euro, oppure fino al 4% del fatturato annuo mondiale dell'esercizio

[63] gdpr.eu. (n.d.). *What is GDPR, the EU's new data protection law?* https://gdpr.eu/what-is-gdpr/

precedente, a seconda di quale cifra sia maggiore. Mentre, violazioni meno gravi, possono comunque essere sanzionate con multe fino a 10 milioni di euro o il 2% del fatturato annuo. [64]

Nel paragrafo 1.4.3 si è visto quanto possono essere elevate le sanzioni e come questo possa incidere in modo significativo non solo sul bilancio delle aziende, ma anche sulla loro reputazione e fiducia degli stakeholder.

Il GDPR ha quindi introdotto responsabilità concrete e significative per le imprese, spingendo il vertice manageriale a considerare la protezione dei dati una priorità strategica e non solo legale.

### 1.7.2 Direttiva NIS2 (Network and Information Security 2)

La Direttiva NIS2 (UE 2022/2555) rappresenta l'evoluzione della prima direttiva NIS del 2016, nel quadro degli sforzi europei per garantire un elevato livello comune di cybersicurezza. NIS2 nasce in risposta all'aumento di minacce cyber verso infrastrutture critiche e servizi essenziali, e mira ad armonizzare e potenziare i requisiti di sicurezza informatica in tutti gli Stati membri, i quali, entro ottobre 2024 hanno dovuto recepirla nelle rispettive legislazioni nazionali, uniformando così i diversi quadri normativi.

Una novità di questa Direttiva, rispetto alla precedente versione, riguarda l'estensione drastica del campo di applicazione. Come già accennato precedentemente, la nuova norma copre molti più settori, passando da circa 20 mila organizzazioni coinvolte con NIS1 a una platea stimata di oltre 300 mila entità soggette a NIS2. Tra queste rientrano settori come l'aerospazio, la pubblica amministrazione, la gestione dei rifiuti, le poste e i corrieri, l'industria chimica e l'agroalimentare, la manifattura di macchinari, la ricerca scientifica, i fornitori di servizi cloud e molti altri. In pratica viene superata la distinzione precedente tra "Operatori di Servizi Essenziali" e "Fornitori di Servizi Digitali", con la conseguenza che le organizzazioni in ambito NIS2 vengono classificate come "Entità Essenziali" o "Entità Importanti", in base al settore in cui operano e alle dimensioni aziendali.

[64] gdpr.eu. (n.d.). *What are the GDPR Fines?* https://gdpr.eu/fines/

Dunque, tra le "Entità Essenziali" rientrano le imprese di settori altamente critici con oltre 250 dipendenti o fatturato maggiore di 50 milioni di euro; mentre, le altre imprese nei settori critici con più di 50 dipendenti e oltre 10 milioni di euro di fatturato, sono considerate "Entità Importanti". Questa categorizzazione impatta soprattutto sulla vigilanza, in quanto le entità essenziali saranno soggette a controlli periodici proattivi, mentre per le importanti la supervisione avverrà principalmente in caso di sospette violazioni. In aggiunta, come nel GDPR, la Direttiva adotta un criterio di applicazione extra-territoriale, in cui anche fornitori esterni all'UE che offrono servizi all'interno, rientrano nel suo ambito. [65]

Un'altra novità rispetto alla NIS1 sono i requisiti più dettagliati e stringenti in termini di misure di cybersecurity da implementare. Tutte le entità interessate dovranno adottare un approccio di gestione del rischio informatico integrato, mettendo in atto misure tecniche e organizzative adeguate. Tra queste rientrano controlli in ambito di sistemi di controllo degli accessi, gestione delle vulnerabilità e aggiornamenti di sicurezza, politiche di formazione del personale, utilizzo della crittografia per proteggere i dati, misure di prevenzione e rilevamento delle intrusioni, piani di risposta e ripristino in caso di incidenti, e tanto altro. Le imprese dovranno quindi formalizzare policy e procedure interne su questi aspetti e documentare periodicamente lo stato di attuazione delle misure. In aggiunta, vi è una particolare attenzione sulla sicurezza della supply chain, poiché le organizzazioni dovranno valutare i rischi cyber lungo la propria catena di fornitura ICT e prevedere nei contratti con fornitori obblighi di sicurezza adeguati.

Le ultime due novità riguardano la notifica degli incidenti e le sanzioni da applicare. Per quanto riguarda il primo aspetto, in caso di incidente che abbia un impatto rilevante sulle operazioni, l'organizzazione dovrà inviare una prima comunicazione entro 24 ore da quando viene a conoscenza dell'evento, indicando le informazioni essenziali. Successivamente entro 72 ore dovrà seguire una notifica completa con dettagli sull'incidente, le cause e le misure di mitigazione adottate. Infine, non oltre 1 mese dalla

[65] Werry, S., Ridgway, W. E., Simon, D. A., Kerr-Shaw, N., & Éles, K. (2024, 11 ottobre). *Navigating the new cybersecurity landscape: Key implications of the EU's NIS 2 Directive*. Skadden, Arps, Slate, Meagher & Flom LLP. https://www.skadden.com/insights/publications/2024/10/navigating-the-new-cybersecurity-landscape

prima segnalazione, dovrà essere inviata un'ulteriore relazione finale con l'analisi post-incidente. La mancata notifica o i ritardi ingiustificati saranno considerati inadempienze sanzionabili. Pertanto, sul fronte delle sanzioni pecuniarie, la Direttiva richiede agli Stati membri di stabilire multe efficaci, proporzionate e dissuasive in linea con quelle del GDPR. Vengono stabiliti importi massimi uniformati, che ammontano per le violazioni commesse dalle entità essenziali fino a 10 milioni di euro o al 2% del fatturato mondiale annuo, mentre per le entità importanti fino a 7 milioni di euro o all'1,4% del fatturato. [66] Queste soglie rappresentano i valori massimi, infatti sarà poi l'autorità nazionale a valutare caso per caso, a seconda della gravità dell'incidente, durata, negligenza o dolo, misure correttive intraprese ecc.

### 1.7.3 DORA (Digital Operational Resilince Act)

Nel settore finanziario, un riferimento normativo di rilievo è il DORA (UE 2022/2554). Si tratta di un regolamento (direttamente applicabile in tutti gli Stati membri senza necessità di recepimento) pensato per assicurare che l'ecosistema finanziario europeo nel suo complesso sia operativamente resiliente di fronte a disservizi o attacchi informatici. L'obiettivo primario è di garantire che banche, assicurazioni, società di investimento, operatori di mercato e altri soggetti finanziari possano resistere, assorbire e riprendersi da eventi avversi di natura ICT, come cyber attacchi, guasti tecnologici o malfunzionamenti di fornitori critici. Come è noto, in assenza di controlli, i rischi informatici nel settore finanziario possono propagarsi a catena e minacciare la stabilità non solo di singoli istituti ma dell'intero sistema economico. [67]

Più nello specifico, il DORA delinea un vero e proprio framework di gestione del rischio ICT integrato nella governance aziendale, disciplinando i seguenti aspetti chiave:

- Gestione del rischio ICT: assicura che ogni unità finanziaria implementi procedure interne per identificare, prevenire e mitigare i rischi informatici. Dunque, implica una chiara definizione dei ruoli e responsabilità a livello di CdA per la resilienza digitale.

[66] Sophos. (s.d.). *What is the NIS2 Directive and compliance?* https://www.sophos.com/en-us/cybersecurity-explained/what-is-the-nis2-directive-faqs
[67] European Insurance and Occupational Pensions Authority. (2024). *Digital Operational Resilience Act (DORA)*. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

- Segnalazioni: gli incidenti ICT dovranno essere segnalati alle autorità competenti (in questo caso la banca centrale o autorità di vigilanza finanziaria) secondo modalità e tempi precisi.
- Test di resilienza operativi digitali: periodicamente le entità finanziarie dovranno testare l'efficacia delle proprie difese cyber.
- Gestione del rischio di terze parti ICT: DORA affronta in modo dettagliato il rischio derivante dai fornitori esterni di servizi ICT, come cloud provider e software. Le entità finanziarie dovranno avere registri aggiornati delle dipendenze da fornitori terzi e valutare il rischio connesso.
- Information sharing: il regolamento incoraggia la creazione di collaborazioni settoriali per la condivisione di informazioni su minacce e incidenti cyber, creando un fronte comune tra operatori. [68]

Si evince che il DORA è un tassello fondamentale della strategia UE per la finanza digitale. Infatti, esso colma le lacune normative emerse in precedenza, dove la resilienza operativa ICT era demandata da linee guida settoriali non uniformi. Ora, con DORA, tutte le entità finanziarie nell'Unione Europea seguono uno standard unico per la sicurezza informatica, elevando il livello medio di preparazione, facendo in modo che gli istituti siano ben preparati a contenere il danno ed evitare che questo possa avere un "effetto domino" sull'economica. Va inoltre sottolineato, che il regolamento è coerente con i principi del NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover), che verranno spiegati nel seguente paragrafo, facilitando l'integrazione con pratiche internazionali già note nel settore finanziario.

### 1.7.4 Framework NIST (Cybersecurity Framework)

Sul versante statunitense, in assenza di normative vincolanti sulla cybersicurezza, ha assunto particolare rilevanza il NIST Cybersecurity Framework (CSF). Fu sviluppato dal National Institute of Standards and Technology (NIST) americano a partire dal 2014, fornendo linee guida volontarie per aiutare organizzazioni di qualsiasi settore a gestire e ridurre il rischio informatico. Pur essendo nato come iniziativa federale USA rivolta

[68] Waterman, D. (2025, 16 gennaio). *Digital Operational Resilience Act (DORA)*. Diligent. https://www.diligent.com/resources/blog/digital-operational-resilience-act-dora

inizialmente alle infrastrutture critiche, il NIST CFS si è dimostrato abbastanza efficace e universale da venire ampiamente adottato a livello globale in vari settori, sia da imprese private che enti governativi. Il framework integra standard e pratiche esistenti (come ISO/IEC 27001, COBIT ecc.) in un approccio strutturato e unificato alla gestione del rischio cyber.

Il cuore del NIST è il Framework Core, che definisce cinque funzioni di alto livello considerate i pilastri di un programma di cybersicurezza efficace. Come mostrato nella Figura 12, tali funzioni sono presentate in forma ciclica a evidenziare la loro interconnessione.


Figura 12: Le cinque funzioni del Framework Core della cybersecurity. Fonte: NIST

Di seguito una descrizione dettagliata di ciascuna delle cinque funzioni:

- Identify (Identificare): significa sviluppare la comprensione organizzativa per gestire il rischio cyber, identificando gli asset critici, le risorse, i dati e i processi vitali, nonché le relative vulnerabilità e minacce.
- Protect (Proteggere): implementare salvaguardie adeguate ad assicurare l'erogazione continua dei servizi critici, includendo maggiori controlli, protezione dei dati, formazione del personale alla sicurezza, manutenzione dei sistemi e utilizzo di tecnologie protettive.
- Detect (Individuare): sviluppare e implementare attività per rilevare tempestivamente il verificarsi di eventi cyber. Ciò implica una capacità di monitoraggio continuo delle reti e dei sistemi, rilevazione di anomalie e possibili violazioni, e appropriate procedure di segnalazioni interne.

- Respond (Rispondere): predisporre attività di reazione efficaci ad eventuali incidenti cyber, ovvero avere piani di risposta ben definiti, team pronti ad intervenire, processi per analizzare l'incidente e contenerlo, comunicazione efficace con gli interessati e le autorità, e capacità di eliminare la minaccia.
- Recover (Recuperare): implementare piani di ripristino e resilienza per riportare tempestivamente le funzioni e i sevizi colpiti allo stato operativo normale dopo un incidente.

Le cinque funzioni del Framework NIST costituiscono un ciclo dinamico e continuo di gestione del rischio, volto a coprire l'intero insieme delle attività di sicurezza a livello strategico e operativo, il tutto in maniera modulare e adattabile in base alle esigenze e al profilo di rischio aziendale. [69]

Un ultimo aspetto su cui soffermarsi è la diffusione del Framework. Benché volontario, il NIST CSF è oggi considerato un punto di riferimento internazionale in materia di cybersicurezza, che va ben oltre i confini statunitensi. Pertanto, è stato tradotto in diverse lingue ed utilizzato da numerose organizzazioni per strutturare i propri programmi di sicurezza, ampliare i requisiti di conformità e viene utilizzato come supporto operativo in Europa per soddisfare le normative come il GDPR, NIS2 e DORA.

### 1.7.5 Altri riferimenti normativi

Oltre alle principali normative e framework trattati sopra, esistono ulteriori riferimenti che contribuiscono a delineare il panorama della cybersecurity a livello internazionale. Tra questi rientrano:

- ISO/IEC 27001: si tratta dello standard internazionale più noto per i sistemi di gestione della sicurezza delle informazioni. ISO/IEC 27001 è una norma volontaria che definisce i requisiti per impostare, implementare, mantenere e migliorare continuamente un programma di sicurezza delle informazioni all'interno di un'organizzazione. Pur non essendo obbligatorio per legge, è ampliamente adottato come riferimento di standard operativo, da cui consegue che

[69] National Institute of Standards and Technology. (2018, 12 aprile). *The CSF 1.1 Five Functions*. https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions

ottenere la certificazione ISO 27001, dimostra ai clienti e partner che l'azienda ha messo in atto un insieme coerente e completo di controlli di sicurezza. Il modello copre aspetti organizzativi e una vasta serie di controlli di sicurezza, dalla gestione degli accessi, alla crittografia, alla sicurezza fisica ecc. Difatti, molte imprese utilizzano la certificazione come base per strutturare i propri controlli per poi mappare tali procedure ai requisiti di normative come GDPR o NIS2. Spesso viene considerato come lo "standard per eccellenza" nell'ambito della sicurezza informatica, in quanto viene riconosciuto globalmente. [70]

- Cyber Resilience Act (CRA): si tratta di una normativa europea rivolta a tutelare consumatori e imprese che acquistano prodotti hardware o software con componenti digitali, affrontando il problema della scarsa sicurezza di molti dispositivi e della mancanza di aggiornamenti tempestivi. Il CRA introduce requisiti obbligatori di cybersicurezza per produttori e rivenditori, che riguardano la pianificazione, la progettazione, lo sviluppo e la manutenzione dei prodotti lungo l'intero ciclo di vita. In quest'ottica, i fabbricanti sono chiamati a garantire non solo la sicurezza iniziale, ma anche la cura e gli aggiornamenti nel tempo. Inoltre, alcune categorie di prodotti particolarmente critici dovranno essere sottoposte a una valutazione di conformità da parte di organismi terzi autorizzati prima di poter essere immesse sul mercato europeo. [71]
- Regolamentazione USA in materia di protezione dei data: come accennato, negli Stati Uniti, non esiste un omologo del GDPR a livello federale. La tutela dei dati personali è affidata a leggi settoriali e statali, facendo prevalere un modello cooperativo/volontario dove gli standard come il NIST CSF fungono da riferimento e le aziende godono di maggiore flessibilità nel come aderirvi.

In definitiva, sebbene l'Europa e gli Stati Uniti adottino approcci differenti, entrambi convergono sull'obiettivo di rafforzare la resilienza digitale e la fiducia degli stakeholder. Per le imprese ciò si traduce non solo in un obbligo di compliance, ma in una leva strategica per tutelare la propria competitività e reputazione nell'economia digitale.

---

[70] Cyberday. (2025, 10 aprile). *Comparing EU cybersecurity frameworks: NIS2, DORA, GDPR and more*. Cyberday Blog. https://www.cyberday.ai/blog/comparing-eu-cybersecurity-frameworks

[71] European Commission. (2025, 6 marzo). *Cyber Resilience Act*. In *Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

**Conclusioni Capitolo 1**

Questo capitolo fornisce tutte le informazioni teoriche del mondo cyber: dalla nascita dei primi sistemi IT e dunque delle prime minacce, al mondo di oggi sempre più interconnesso e con migliaia di vulnerabilità. Si sono inoltre evidenziate le principali conseguenze che un attacco cyber può causare, da quelle con impatto immediato, alle conseguenze più durature e difficili da gestire; ed inoltre, sono state presentate le principali sfide che gli attori delle organizzazioni devono affrontare per conciliare la sicurezza del mondo cyber con la realtà terrestre. Infine, è stato riportato un quadro normativo che include le principali normative a livello europeo, con una digressione sui regolamenti statunitensi al fine di proporre un confronto.

## CAPITOLO 2 – CYBERSECURITY E REPUTAZIONE

In questo capitolo verrà analizzato il legame tra cybersecurity e reputazione, sia a livello aziendale che a livello nazionale, e come un attacco informatico possa influenzare la percezione pubblica e il valore di un *brand*. Per fare ciò, verranno esaminati dei casi di aziende che hanno subito attacchi cyber e come ciò abbia impattato sulla loro posizione di mercato, e si discuteranno le strategie di *reputation management* e comunicazione di crisi specifiche per gli incidenti cyber. [72]

### 2.1 Definizione di reputazione aziendale e importanza strategica

La reputazione aziendale è comunemente intesa come un asset intangibile di fondamentale rilevanza strategica per le organizzazioni moderne. In letteratura esistono varie definizioni autorevoli del concetto. Tra queste, una di Fombrun et el. (2000), in cui la reputazione viene definita come un "*costrutto collettivo che descrive la percezione aggregata di molteplici stakeholder riguardo alla performance di un'azienda*". [73]
In termini simili, Gotsi e Wilson (2001) parlano di reputazione come "*la valutazione complessiva di un'azienda da parte degli stakeholder nel tempo*", basata sulle esperienze dirette che essi hanno con l'azienda e sulle informazioni riguardanti le azioni passate dell'impresa. Mettendo insieme questi due pensieri, la reputazione riflette il giudizio collettivo e comparativo degli attori chiave (clienti, investitori, dipendenti, partner, pubblico) sulla capacità e affidabilità di un'azienda nel soddisfare aspettative ed impegni assunti nel tempo.

Questa natura percettiva e cumulativa della reputazione comporta che si costruisca nel lungo periodo, attraverso un insieme di segnali e comportamenti aziendali osservati dagli stakeholder. Inoltre, la reputazione differisce dall'immagine o dal marchio, poiché rappresenta un giudizio consolidato e multi-divisionale sulla credibilità, affidabilità e la stima complessiva di cui gode l'impresa presso i suoi pubblici di riferimento. Wartick

[72] **World Economic Forum.** (n.d.). *Cyber risk leadership and corporate governance*. https://www.weforum.org/projects/cyber-risk-leadership-and-corporate-governance/
[73] Özbağ, G. K., & Çekmecelioğlu, H. G. (2019). Examining the effects of dimensions of corporate reputation on firm performance. *The European Proceedings of Social & Behavioural Sciences (EpSBS)*, *LXIV*, 271–280.

(1992), ad esempio, la descrive come "*l'aggregazione delle percezioni di un singolo stakeholder su quanto le risposte organizzative soddisfano le aspettative di molteplici stakeholder*", enfatizzando così la molteplicità di prospettive che confluiscono nella reputazione.

Ma come si traducono queste minacce nella realtà operativa di imprese e istituzioni?
Dal punto di vista del management strategico, la reputazione aziendale è riconosciuta come una risorsa intangibile preziosa e difficilmente imitabile, in grado di generare un vantaggio competitivo durevole. Infatti, secondo la Resource-Based View (RBV) delle imprese, solo le risorse rare, non facilmente sostituibili e non imitabili possono produrre performance superiori nel tempo. La reputazione risponde a questi requisiti in quanto è il frutto di anni di buone performance e comportamenti coerenti, non si può acquistare sul mercato e può essere facilmente danneggiata, ma non difficilmente ricostruita. Pertanto, Hall (1993) la definisce come "*il più importante asset intangibile*" di un'azienda proprio per queste ragioni. Di conseguenza, un'ottima reputazione consente di ottenere benefici tangibili: le imprese più stimate possono praticare prezzi premium, attrarre e fidelizzare più clienti, ridurre i costi di transazione, assicurarsi maggiore fiducia da parte degli investitori e reclutare dipendenti di talento e condizioni più vantaggiose. In questo modo, la reputazione positiva funziona da "scudo competitivo", creando barriere all'entrata e proteggendo la redditività nel lungo periodo. Di fatto, è stato studiando come le aziende con reputazione elevata abbiamo migliori performance finanziarie nel breve e lungo periodo. Parallelamente a ciò, alcuni dati indicano anche che la reputazione costituisce una quota significativa degli asset intangibili, arrivando a rappresentare circa il 63% del valore di mercato di un'organizzazione. [74] Inoltre, il Reputational Institute ha calcolato che, in media, una variazione di 1 punto nel punteggio RepTrak (indice reputazionale che verrà approfondito in seguito) corrisponde a circa il 2,6% di variazione nel valore di mercato dell'impresa. [75] Questi dati confermano quantitativamente quanto la reputazione sia un vero e proprio driver di valore aziendale.

[74] **PR Newswire.** (2019, ottobre 30). *Reputation accounts for 63 percent of a company's market value*. https://www.prnewswire.com/news-releases/reputation-accounts-for-63-percent-of-a-companys-market-value-300986105.html
[75] Poma, L. (2023, 24 febbraio). *"Fake reputation": come manipolare il più prezioso degli asset intangibili di un'organizzazione*. *Creatori di Futuro*. https://creatoridifuturo.it/articoli-luca-poma/fake-reputation-come-manipolare-il-piu-prezioso-degli-assets-intangibili/

Dunque, la reputazione aziendale è un costrutto multidimensionale e dinamico, frutto dell'aggregazione delle percezioni degli stakeholder sulle capacità dell'impresa di mantenere le proprie promesse e comportarsi in modo coerente con aspettative economiche, etiche e sociali. D'altro canto, se la reputazione dovesse essere compromessa, ciò esporrebbe l'organizzazione a rischi strategici notevoli, in quanto l'erosione della fiducia degli stakeholder e la perdita di sostegno del mercato possono tradursi rapidamente in danni economici concreti.

### 2.2 Cyber risk e conseguenze sulla reputazione e la fiducia degli stakeholder

Come è stato evidenziato del Capitolo 1, attacchi informatici gravi, non comportano solo costi tecnici e operativi, ma possono minare profondamente la fiducia di clienti, investitori e altri stakeholder chiave. Non a caso, il recente sondaggio Global Reputational Risk Readiness Survey 2024/5 ha evidenziato come su 500 dirigenti senior il 65% dei manager identifichi gli attacchi cyber come il principale rischio per la reputazione aziendale, superando anche altri pericoli come le problematiche ambientali o di governance. [76]

Nella Figura 13 si può osservare come tale percentuale sia aumentata drasticamente rispetto agni anni passati, dimostrando una crescente consapevolezza dell'impatto reputazionale degli incidenti informatici.

[76] **Willis, a WTW Business. (2025, maggio 27).** *65 % of global corporate risk strategists identify cyber-attacks as the most significant threat to reputation, according to latest Willis survey* [Press release]. WTW. https://www.wtwco.com/en-gb/news/2025/05/65-percent-of-global-corporate-risk-strategists-identify-cyber-attacks-as-the-most-significant#:~:text=LONDON%2C%20May%2027%2C%202025

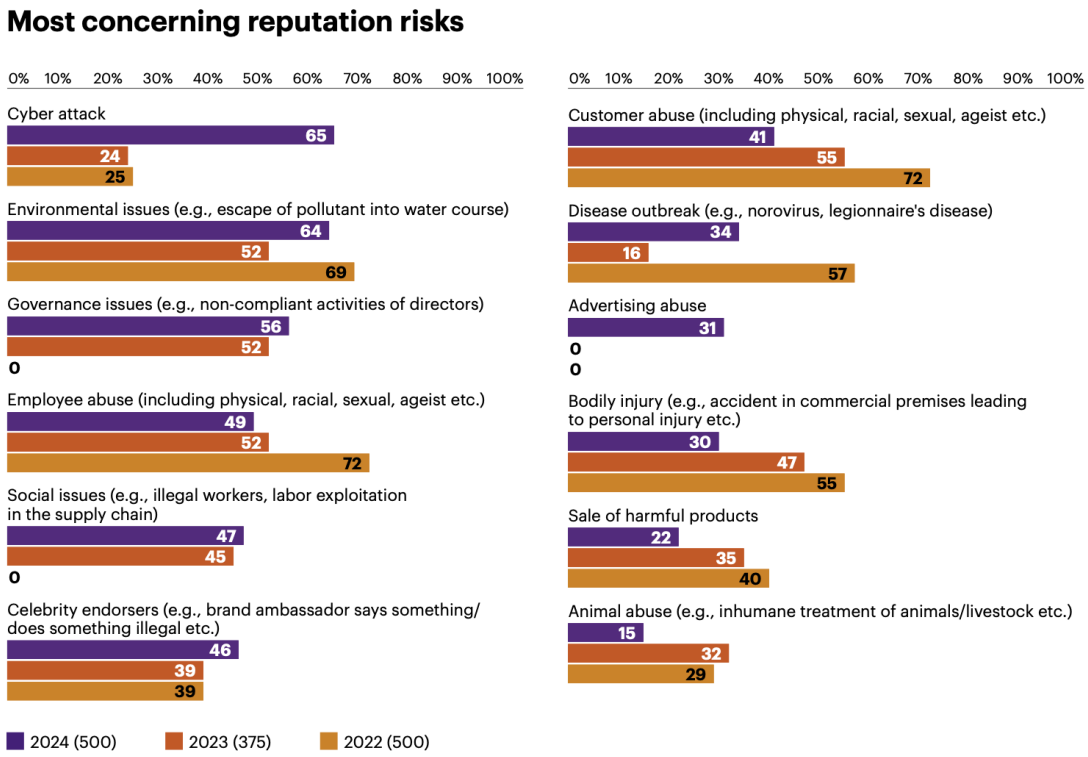



Figura 13: Rischi reputazionali più preoccupanti per le imprese nel mondo (2022-2024). Fonte: Global Reputational Risk Readiness Survey 2024/5

Ma come incide concretamente un attacco informatico sulla reputazione e sulla fiducia?

### 2.2.1 Reazione clientela

In primo luogo, vi è un immediato effetto di shock sulla fiducia dei clienti. Quando vengono sottratti o compromessi dati personali sensibili (numeri di carte di credito, informazioni finanziarie, dati sanitari, credenziali di accesso, ecc.), i clienti si sentono "traditi" nelle proprie aspettative di riservatezza e sicurezza.

Ad esempio, uno studio di McKinsey sul tema "privacy e consumatori" rivela che ben l'87% dei consumatori non farebbe più affari con un'azienda se ha dubbi sulle sue pratiche di sicurezza, e il 71% interromperebbe immediatamente la relazione

commerciale se scoprisse che l'azienda ha gestito in modo improprio o "ceduto" i propri dati sensibili senza autorizzazione. [77]

In aggiunta, il report Cyber Readiness Report 2024 pubblicato da HISCOX, fornisce ulteriori numeri concreti e significativi:

| Impacts of cyber attacks in the past 12 months | 2024 % | 2023 % |
|---|---|---|
| Greater difficulty attracting new customers | **47** | 20 |
| Lost customers | **43** | 21 |
| Bad publicity, which impacted brand reputation | **38** | 25 |
| Lost business partners | **21** | 16 |

Figura 14: Effetti dei cyber attacchi sulle imprese negli ultimi 12 mesi: confronto tra 2023 e 2024(%). Fonte: Cyber Readiness Report 2024

Si può osservare che tra le aziende colpite da attacchi cyber, il 47% ha riscontrato difficoltà ad acquisire nuovi clienti dopo l'evento, il 43% ha perso clienti esistenti, ed il 38% ha subito danni di cattiva pubblicità sui media. [78] Si tratta di aumenti notevoli rispetto all'anno precedente, a conferma del fatto che gli attacchi informatici stanno diventando uno dei principali inneschi di perdita di fiducia per le imprese.

Queste evidenze empiriche dimostrano che la reazione istintiva di molti clienti di fronte a una violazione, è quella di considerare l'azienda inaffidabile, portandoli a migrare verso concorrenti ritenuti più sicuri, mettendo in risalto quanto la fedeltà del cliente risulti fragile. Per lo più, la perdita di fiducia può manifestarsi anche con danni al marchio: brand un tempo forti e solidi possono improvvisamente essere associati a negligenza o scarsa tutela degli utenti, con un calo di sentiment generale espresso dai clienti sia nelle indagini di soddisfazione sia nelle conversazioni sui social media.

[77] **Anant, V., Donchak, L., Kaplan, J., & Soller, H.** (2020, April 27). *The consumer-data opportunity and the privacy imperative*. McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

[78] Hiscox Group. (2024, ottobre). *Cyber Readiness Report 2024: Protecting reputation through cyber resilience* (HSX245). https://www.hiscoxgroup.com/sites/group/files/documents/2024-10/HSX245%20–%202024%20CRR.pdf

### 2.2.2 Reazione mercati finanziari

Allo stesso tempo, anche gli investitori reagiscono negativamente alle notizie di cyber attacchi, anticipando conseguenze economiche e di reputazione. Numerosi studi in finanza mostrano che gli annunci pubblici di una violazione di sicurezza portano spesso a ribassi significativi del titolo azionario dell'azienda colpita, quantificando in modo immediato il "costo reputazionale" percepito dal mercato. [79]

Secondo un'ampia analisi condotta da Comparitech su 118 aziende quotate colpite da un *data breach*, in media le azioni delle società subiscono un calo modesto ma misurabile: circa il -1,4% del valore di picco, raggiunto intorno a 41 giorni dopo la divulgazione pubblica dell'incidente. [80] Questo impatto medio contenuto suggerisce che i mercati azionari spesso "assorbono" rapidamente la notizia di una violazione, soprattutto se l'azienda comunica subito ed efficacemente il problema. Tuttavia, esistono casi estremi in cui il danno reputazionale percepito dagli investitori è molto più elevato. Esempio emblematico già citato è quello relativo ad Equifax, in cui il titolo crollò del -60% nelle settimane successive, recuperando solo dopo molti mesi. Anche società come Yahoo! e SolarWinds videro calare le loro azioni rispettivamente del -3,8% e -40% nel giro di poche settimane.

Da queste affermazioni, emerge dunque, che un attacco informatico grave può innescare un circolo vizioso reputazionale: i media diffondono la notizia amplificando l'eco negativo sull'azienda, di conseguenza gli stakeholder reagiscono con indignazione o preoccupazione e la fiducia viene meno, causando comportamenti penalizzanti.

## 2.3 Casi concreti di impatto reputazionale dovuti a cyber eventi

Per capire al meglio le conseguenze reputazionali ed avere una percezione più reale di quanto detto fino ad ora, nel seguente paragrafo verranno analizzati quattro casi rappresentativi che mostrano come i cyber attacchi possono colpire duramente la fiducia e l'immagine di aziende ed istituzioni, in diversi settori e contesti. Le realtà analizzate

[79] Wang, P., & Park, S.-A. (2017). *Communication in cybersecurity: A public communication model for business data breach incident handling*. *Issues in Information Systems, 18*(2), 136–147.
[80] Bischoff, P. (2024, 5 giugno). *How data breaches affect stock market share prices*. Comparitech. https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/

appartengono infatti ad ambiti eterogenei, circostanza che permette di evidenziare la varietà con cui le conseguenze degli attacchi possono manifestarsi in relazione al settore di riferimento e alle peculiarità dell'organizzazione coinvolta.

### 2.3.1 Caso SolarWinds

Uno dei primi grandi scandali degli anni recenti è la compromissione di SolarWinds, emersa nel 2019. SolarWinds è una società fornitrice di software di monitoraggio di rete (in particolare la piattaforma Orion), usata da migliaia di organizzazioni nel mondo, incluse numerose agenzie governative statunitensi. L'attacco, attribuito a un gruppo APT legato all'intelligence russa, ha avuto la forma di un attacco alla supply chain. Più nel dettaglio, i criminali informatici sono riusciti a inserire un malware all'interno di un aggiornamento legittimo del software Orion, distribuito poi ai clienti di SolarWinds. In questo modo, gli attaccanti hanno indirettamente ottenuto l'accesso alle reti di 18.000 organizzazioni che installarono l'aggiornamento compromesso, tra cui il Dipartimento del Tesoro USA, grandi aziende tecnologiche e molto altre. Si tratta di uno degli attacchi più sofisticati e pericolosi degli ultimi anni, con implicazioni di sicurezza nazionale. [81]

Dal punto di vista reputazionale, l'impatto su SolarWinds è stato immediato e gravissimo. Prima dell'incidente, la società godeva di una reputazione solida come fornitore affidabile di strumenti IT; ma in seguito è stata travolta dalle critiche per non aver saputo prevenire né rilevare per tempo l'intrusione nei propri sistemi.
In particolare, è emerso come gli hacker avessero avuto accesso alle infrastrutture del software per molti mesi senza essere scoperti, e che alcune pratiche interne di sicurezza fossero gravemente inadeguate. Per esempio, il caso divenuto simbolico è quello di una password interna "solarwinds123" lasciata in chiaro su un server, già segnalata in passato. Dunque, questi elementi hanno dipinto l'azienda come negligente sulla cybersecurity, scatenando un'ondata di sfiducia. Fonti di settore riportano che il titolo azionario crollò del 40% nella settimana successiva alla rivelazione dell'attacco, dimostrando sfiducia da parte degli investitori preoccupati sia dai costi che dai danni di reputazione.

[81] Ollis/Akers/Arney Insurance & Business Advisors. (2021). *Cyber case study: SolarWinds supply chain cyberattack*[PDF]. Zywave, Inc. https://ollisakersarney.com/wp-content/uploads/2021/10/Cyber_Case_Study_-_SolarWinds_Supply_Chain_Cyberattack.pdf

L’azienda si è trovata al centro di un caso mediatico e politico: oltre al danno d’immagine commerciale, vi è stato un danno di reputazione istituzionale poiché l’episodio ha messo in discussione la fiducia nella filiera ICT americana. Come conseguenza, SolarWinds ha affrontato anche ripercussioni legali e indagini regolatorie da parte della SEC (Securities and Exchange Commission) sulla comunicazione dell’incidente.
In risposta, la società ha tentato un impegnativo percorso di rebranding e rafforzamento delle pratiche di sicurezza, assumendo esperti di cybersecurity di alto profilo e cambiando nome al software compromesso. Ma, nonostante queste operazioni, a distanza di anni il caso SolarWinds rimane un esempio di come un singolo attacco possa minare radicalmente la reputazione costruita in decenni.

### 2.3.2 Caso Colonial Pipeline

Un altro caso eclatante è l’attacco ransomware subito da Colonial Pipeline nel 2021. La società in questione gestisce uno dei maggiori oleodotti negli Stati Uniti, che rifornisce circa il 45% del carburante della costa Est.
Nel maggio del 2021, un gruppo di hacker, conosciuto come “DarkSide”, ottenne l’accesso al network di Colonial Pipeline attraverso una password VPN compromessa. Una volta dentro, gli hacker esfiltrarono circa 100 GB di dati e distribuirono ransomware che cifrò parte dei sistemi, inducendo Colonial a fermare preventivamente le operazioni dell’intero oleodotto per alcuni giorni, al fine di contenere la minaccia. Questa interruzione operativa, sebbene motivata da precauzione, ebbe immediatamente un impatto enorme: si verificarono carenze di carburante che generarono panico lungo tutta la costa Sud ed Est, facendo aumentare i prezzi della benzina a livelli massimi. Vista la situazione critica, il Governo federale dichiarò lo stato di emergenza e dovette intervenire per garantire forniture alternative al ripristino. Colonial Pipeline decise anche di pagare un riscatto di 75 bitcoin ai criminali, nel tentativo di accelerare il ripristino dei sistemi, ma così facendo creò solamente un’opinione pubblica ancora più negativa.

L’impatto reputazionale per Colonial Pipeline si manifestò su più livelli. In primo luogo, la scelta di pagare il riscatto venne fortemente criticata da esperti e forze dell’ordine, alimentando la narrativa che l’azienda avesse finanziato i cybercriminali e incentivato futuri attacchi. La conseguenza fu che Colonial fu percepita come vulnerabile e priva di

preparazione adeguata. In secondo luogo, l'interruzione del servizio ha reso tangibile al grande pubblico il legame tra cybersecurity e vita quotidiana: milioni di cittadini si sono trovati senza benzina, sviluppando di riflesso un'immagine negativa dell'azienda che non ha saputo "proteggere" un'infrastruttura così fondamentale.

I media coprirono la vicenda a 360 gradi, enfatizzando il senso di vulnerabilità sistemica, inferendo un duro colpo alla reputazione di Colonial Pipeline a livello di pubblica opinione.

Mentre, sul fronte legale, la società ha affrontato anche una class action da parte di clienti (ad esempio distributori di carburante) e indagini federali, alimentano ulteriormente la stampa negativa e dunque la percezione collettiva.

Ne consegue che, questo caso evidenzia come un attacco informatico su infrastrutture critiche abbia un duplice impatto reputazionale: interno al settore (fiducia degli stakeholder diretti) ed esterno, generando panico e perdita di fiducia a livello di giudizio comune ed istituzioni. La vicenda ha infatti accelerato iniziative governative per imporre standard di sicurezza più stringenti alle infrastrutture energetiche, segno che la reputazione all'interno dell'ecosistema era stata danneggiata. [82]

### 2.3.3 Caso Travelex

Il caso Travelex rappresenta un esempio di come un attacco informatico possa contribuire a mandare in crisi irreversibile un'azienda. Questa società è nota per essere stata fornitrice di servizi di cambio valuta con presenza globale (con oltre 1.200 sportelli in aeroporti e città turistiche).

La notte di Capodanno del 2019, Travelex subì un attacco ransomware che costrinse l'azienda ad interrompere tutti i sistemi IT e il sito web a livello mondiale. Per giorni, l'operatività fu garantita solo manualmente, ovvero il personale dovette tornare ad operare con carta e penna per registrare le transazioni, creando disservizi enormi in piena stagione di viaggi.

Nel frattempo, gli hacker minacciavano di pubblicare 5GB di dati rubati, tra cui informazioni personali di clienti, chiedendo un riscatto di circa 6 milioni di dollari.

[82] INSURICA. (2025, 25 aprile). *Cyber case study: Colonial Pipeline ransomware attack*. https://insurica.com/blog/colonial-pipeline-ransomware-attack/

La situazione si protrasse per settimane, assistendo ad un impatto a cascata su numerose banche partner che dovettero sospendere i propri servizi di cambio online a causa dell'indisponibilità di Travelex. Questo creò un "effetto domino" reputazionale: non solo Travelex appariva in difficoltà, ma anche le banche clienti si trovarono esposte a lamentele dei propri utenti per disservizi, scaricando ulteriormente pressione sulla società.

Dunque, le conseguenze reputazioni furono devastanti. Innanzitutto, il fatto che un attacco del genere avvenisse in un periodo festivo è stato molto penalizzante ed ha evidenziato come i criminali tendono a scegliere momenti in cui le difese aziendali sono potenzialmente meno pronte.
Travelex fu criticata per non aver aggiornato software critici e per essere stata lenta e poco trasparente nella comunicazione. Infatti, inizialmente i messaggi sul sito parlavano di "manutenzione programmata" invece di ammettere il cyber attacco, scelta che poi ha aggravato la percezione di scarsa sincerità e controllo della situazione. Per di più, molti clienti rimasero senza denaro o con transazioni bloccate, esprimendo pubblicamente il proprio malcontento, lamentando una gestione caotica e scarsa assistenza. Gli osservatori notarono che l'attacco aveva provocato danni di immagine sia verso i consumatori finali, che verso le istituzioni finanziarie partner, incrinando la fiducia dell'affidabilità di Travelex come fornitore B2B. [83]
Dal punto di vista finanziario, la casa madre Finablr inizialmente minimizzò l'impatto economico, ma dovette rapidamente rivedere le stime, che misero in evidenza una perdita di circa 25 milioni di sterline in utile operativo direttamente imputabile all'attacco mentre il prezzo delle azioni di Finablr subì un calo e alcuni investitori disinvestirono, segnalando pessime aspettative sul recupero di Travelex. [84]
Parallelamente ai danni economici del ransomware e il contraccolpo reputazionale, un ulteriore aspetto che indebolì l'azienda fu il Covid-19 che azzerò il mercato dei viaggi, portando Travelex a dichiarare la bancarotta con il taglio di oltre 1.000 posti di lavoro.

[83] OnSecurity Team. (2020, 13 ottobre). *Cyber Nightmare: What went wrong with Travelex and why?* OnSecurity. https://www.onsecurity.io/blog/cyber-nightmares-what-went-wrong-with-travelex/
[84] Riskonnect. (2025, 31 gennaio). *Cost and consequences of Travelex hack could run and run*. https://riskonnect.com/cyber-security/industry-news-cost-and-consequences-of-travelex-hack-could-run-and-run/

Il caso Travelex dimostra come un incidente cyber possa fungere da catalizzatore di una crisi letale per un'azienda già indebolita, erodendone la reputazione e la capacità di risollevarsi. Dal punto di vista regolatorio, l'azienda rischiò anche pesanti sanzioni GDPR per la mancata notifica tempestiva dell'incidente, ulteriore elemento che avrebbe colpito l'immagine di compliance dell'azienda. In definitiva, Travelex è un caso citato per evidenziare che i costi intangibili di una violazione, come la perdita di fiducia dei clienti, la rottura di relazioni con partner, pubblicità negativa, ed anche periodi difficili come il Covid-19, possono superare quelli tangibili ed immediati, condurre alla chiusura dell'attività e alle conseguenze acquisizione da parte dei creditori.

### 2.3.4 Caso Vastaamo

L'ultimo caso, forse il più grave dal punto di vista umano, è quello di Vastaamo. Si tratta di una clinica privata finlandese di psicoterapia, vittima di un attacco senza precedenti per modalità e impatto sociale. Nel 2020, la società ha rivelato pubblicamente che il suo intero database di cartelle cliniche di pazienti (circa 36.000 persone) era stato violato da hacker non identificati già da tempo. Gli aggressori avevano rubato dati estremamente sensibili, come appunti delle sedute di terapia, diagnosi, dati personali dei pazienti, compresi minorenni. Ma ciò che rese il caso particolarmente contorto fu la strategia di doppia estorsione adottata: inizialmente i criminali chiesero un riscatto di 40 bitcoin (circa 45.000€) alla clinica per non pubblicare le informazioni; però, nel frattempo, per fare pressione, iniziarono a pubblicare giornalmente su forum del dark web piccoli lotti di dati di pazienti. Poiché l'azienda non cedette, gli hacker passarono al secondo ricatto, ovvero inviarono e-mail individuali a migliaia di pazienti, chiedendo a ciascuno un piccolo riscatto personale per evitare la diffusione dei propri verbali di terapia. Pertanto, le vittime, già vulnerabili, si trovarono doppiamente vittimizzate: da un lato attraverso l'invasione della propria privacy, dall'altro attraverso il ricatto diretto.

Mentre l'incidente scioccò l'intero paese, tanto da far richiamare una riunione straordinaria del governo e costando il posto al CEO di Vastaamo, le sue ripercussioni potrebbero estendersi ben oltre i confini della Finlandia. Infatti, la questione riguarda sia gli obblighi delle organizzazioni sanitarie nel proteggere le proprie reti informatiche, sia

la possibilità delle vittime di chiedere conto alle organizzazioni stesse delle loro mancanze in tal senso. [85]

Le conseguenze in termini di reputazione e fiducia sono state profonde e molteplici.
Per prima cosa è emerso che le pratiche di sicurezza informatica di Vastaamo erano gravemente negligenti, tanto da non avere i dati clinici cifrati nel database e da non avere alcuna password di accesso al server.
Per giunta, come sottolinea la psichiatra statunitense Ryan Louie, in questo caso non si parla solo di cybersicurezza, ma di un vero e proprio attacco diretto alla "*psybersecurity*", ovvero un concetto molto più ampio che richiama l'importanza di sentirsi protetti non solo a livello digitale, ma anche nella propria salute mentale all'interno del mondo online. [86]

Mentre, in termini di reputazione aziendale, si può affermare che la società è divenuta sinonimo di irresponsabilità, facendo perdere la fiducia da parte di pazienti e partner, portando a dichiarare bancarotta nel 2021, cedendo le attività rimanenti ad altri operatori. In questo caso sarebbe stato difficile immaginare un futuro diverso, in quanto nessuno mai avrebbe più usufruito del servizio di psicoterapia dopo uno scandalo simile. In aggiunta, dopo l'accaduto, la società finlandese si scusò pubblicamente e mise a disposizione servizi di supporto, ai quali si affiancò in modo significativo l'iniziativa di un gruppo di volontari composto da professionisti del settore, che pubblicarono guide per aiutare le vittime a riprendersi dalla violazione, includendo anche raccomandazioni legate al benessere mentale e psicologico. Pertanto, questo evento dimostra una risposta comunitaria al problema, percepito come un vero e proprio attacco alla società nel suo insieme.
Infine, in termini di reputazione nazionale, questo episodio ha sicuramente costretto la Finlandia, nota per la sua affidabilità e sicurezza digitale, a rivedere gli standard di sicurezza nel settore sanitario e a migliorare la gestione dei dati sensibili per evitare incidenti simili in futuro. [87]

---

[85] Lyngaas, S. (2020, 29 ottobre). *Why the extortion of Vastaamo matters far beyond Finland — and how cyber pros are responding*. CyberScoop. https://cyberscoop.com/finland-vastaamo-hack-response/
[86] Lyngaas, S. (2020, 29 ottobre). *Why the extortion of Vastaamo matters far beyond Finland — and how cyber pros are responding*. CyberScoop. https://cyberscoop.com/finland-vastaamo-hack-response/
[87] Ghanbari, N., & Koskinen, J. (2024). *When data breach hits a psychotherapy clinic: The Vastaamo case*. Helsinki University. https://doi.org/10.31885/aa.2024.6

In definitiva, i casi analizzati contribuiscono a concretizzare quanto spiegato nei paragrafi teorici relativi ai danni e alle possibili conseguenze, mostrando in modo reale e tangibile come il danno reputazionale rappresenti una componente inevitabile nei gravi attacchi informatici.

## 2.4 Strumenti e metriche per misurare la reputazione e i danni reputazionali dopo un attacco informatico

Misurare in modo oggettivo la reputazione aziendale è una sfida complessa, che verrà riscontrata anche durante l'analisi empirica di questo elaborato, data la natura multidimensionale e percettiva del concetto. Nel corso del tempo sono stati sviluppati numerosi strumenti e metriche per quantificare la reputazione e monitorarne l'andamento, sia per fini accademici che operativi. Tali misure si possono suddividere in due macrocategorie: da un lato gli approcci basati sulle percezioni dirette degli stakeholder (come sondaggi e indici compositi di immagine), dall'altro quelli basati su indicatori indiretti o proxy quantitative (ad esempio performance finanziarie, indicatori di mercato e la narrativa mediatica).
Di seguito verranno esaminati in modo più approfondito.

### 2.4.1 Valutazione dell'esperienza dei clienti mediante indagini strutturate e analisi del sentiment

Il primo approccio analizzato è quello che coinvolge direttamente i clienti e la loro esperienza con l'azienda e i suoi servizi. Molte imprese, in particolare quelle B2C, monitorano costantemente il livello di soddisfazione e di fiducia della propria clientela attraverso vari strumenti, tra cui il Customer Satisfaction Score (CSAT), il Trust Index, il Net Promoter Score (NPS) e altri questionari finalizzati a misurare il grado di soddisfazione percepita. I dati mostrano come tali indicatori tendano a diminuire sensibilmente in seguito ad un attacco informatico.

Con la crescente dipendenza dai dispositivi elettronici, l'aumento dei dati sensibili condivisi dagli utenti e il parallelo incremento di attacchi informatici, cresce anche la

preoccupazione delle persone per la propria sicurezza digitale. Un recente studio finalizzato da Deloitte afferma quanto detto: il 58% dei consumatori si dichiara più preoccupato di prima riguardo alla sicurezza dei propri dati presso le aziende digitali, evidenziando un clima di fiducia già precario che può essere ulteriormente compromesso anche da un singolo incidente. [88]
Ne consegue che, a seguito di un data breach, gli indici citati precedentemente e la soddisfazione generale dei clienti potrebbe calare bruscamente, impattando anche la fiducia nel settore tecnologico e nell'azienda violata.

Un altro indicatore indiretto, ma significativo, è il volume di richieste di supporto o reclami ricevuti dall'impresa dopo un incidente. Di fatto, un picco di segnalazioni di clienti spaventati per i propri dati e malcontenti per il disservizio, sono un segno di danno reputazionale in atto. Questo può essere ricollegato a quanto si è visto nel caso Vastaamo, nel momento in cui l'azienda dovette fornire assistenza telefonica per supportare psicologicamente le vittime dell'incidente, mostrando un chiaro simbolo della profonda rottura di fiducia.

In aggiunta, con l'avvento della *data analytics* e l'intelligenza artificiale, si sono diffusi strumenti innovativi per monitorare la reputazione in tempo reale, come l'analisi del sentiment sui media e social network. Attraverso specifici algoritmi come il *text mining* e *Natural Language Processing*, è possibile quantificare la tonalità delle discussioni (positive, neutre, negative) pubbliche e della copertura mediatica relativa ad un'azienda. Ad esempio, in caso di attacco informatico, si può misurare l'esposizione di menzioni negative sui social e sui notiziari, e usare tale indicatore come misura del danno reputazionale immediato. Questo tipo di analisi può fornire un riscontro quasi istantaneo della percezione pubblica, sebbene vada interpretato con cautela e normalizzato rispetto al livello di notorietà pregresso del marchio. [89]

[88] Deloitte Insights. (2023, 5 settembre). *Consumer data privacy and security*. In *Connectivity & Mobile Trends Survey 2023*. https://www.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey/2023/data-privacy-and-security.html
[89] Colleoni, E., Arvidsson, A., Hansen, L. K., & Marchesini, A. (2011). *Measuring Corporate Reputation using Sentiment Analysis*. Paper presented at the 15th International Conference on Corporate Reputation, New Orleans, United States.

Più nel dettaglio, strumenti di *social listening* avanzati permettono di segmentare le conversazioni per tema e identificarne le opinioni principali, fornendo informazioni utili per modulare la risposta comunicativa. Le aziende più all'avanguardia gestiscono la reputazione come un vero rischio operativo. Infatti, come raccomandato da un noto manager Garret Gaughan: "Per costruire resilienza le imprese dovrebbero sviluppare solidi processi di risk management, inclusi il monitoraggio del *sentiment* e l'*intelligence* sui rischi". Ciò implica dotarsi di piattaforme di reporting in tempo reale che aggregano indicatori reputazionali e procedure di allerta quando si rivela un anomalo incremento di negatività nelle conversazioni sul brand.

### 2.4.2 Andamento del valore azionario

Come si è già visto nei casi analizzati, per le società quotate, il prezzo delle azioni riflette in modo immediato il sentiment degli investitori. Infatti, un calo anomalo del titolo all'annuncio di un cyber attacco indica che il mercato sta scontando non solo i costi diretti, ma anche un potenziale deterioramento di fiducia e prospettive future. Tuttavia, l'effetto di una violazione di dati sul valore delle azioni varia in base al settore e all'organizzazione colpita, alla dimensione della violazione e al tipo di dati sottratti.

Riprendendo quanto detto riguardo la ricerca svolta da Comparitech sulle 118 aziende quotate, le azioni possono avere un calo di appena -1,4% dopo circa due mesi dall'attacco. Ma non sempre è così. Pertanto, è emerso che i settori che trattano grandi quantità di dati sensibili soffrono più. Ad esempio, le aziende sanitarie hanno "sottoperformato" l'indice NASDAQ di ben -10,6% nei mesi successivi alla violazione, seguite dal settore finanziario e manifatturiero; mentre, il settore del retail ha addirittura sovraperformato, dimostrando che gli investitori sono più sensibili alle organizzazioni che trattano dati ritenuti più personali. [90]

[90] Bischoff, P. (2024, 5 giugno). *How data breaches affect stock market share prices*. Comparitech. https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/

### 2.4.3. Perdita di clienti e quota di mercato

Probabilmente la perdita di clienti è uno degli indicatori più diretti dell'impatto reputazionale. Dopo un incedente cyber, un'azienda può registrare un aumento del tasso di abbandono dei clienti e un calo di nuovi acquisti, dovuti alla diminuzione di fiducia.
Facendo riferimento a quanto evidenziato già nel paragrafo 2.2.1, una delle principali azioni che intraprendendo i clienti dopo un attacco informatico è l'abbandono dei servizi dell'azienda.

Questi dati possono riflettersi in metriche come il numero di account cancellati, il calo di utenti attivi, la diminuzione del volume di vendite o ordini ripetuti nei periodi seguenti, impattando soprattutto le piattaforme e-Commerce. In altri casi, si può misurare attraverso la perdita di contratti o la diminuzione di affari con i partner (come si è analizzato nel caso Travelex). Infine, anche indicatori di traffico web o di utilizzo del servizio prima e dopo l'incidente possono suggerire un impatto reputazionale, indicando che gli utenti non sono più interessati all'utilizzo.

### 2.4.4 Indicatori di brand equity e ranking reputazionali

Esistono apposite classifiche e indici che cercano di misurare la forza del brand e la reputazione di esso.
Tra queste rientra la classifica delle "World's Most Admired Companies" pubblicata dalla rivista Fortune, che sin dagli anni '80 raccoglie il giudizio di dirigenti e analisti su aziende leader, valutate su attributi come innovazione, qualità del management, responsabilità sociale, solidità finanziaria, capacità di attrarre talenti, qualità dei prodotti ecc. Sebbene a fini accademici questa classifica sia stata utilizzata come proxy di reputazione, studi più recenti ne evidenziano i limiti, preferendo metriche più mirate.

Infatti, in ambito accademico, è emersa una certa eterogeneità nelle misure adottate: l'analisi di Bigus et al. (2023) ha dimostrato che 173 studi nei campi di accounting e management mostrano che tutt'oggi vengono impiegati indicatori finanziari secondari, come la dimensione aziendale e la quota di mercato, per misurare la reputazione, specialmente nelle ricerche economico-contabili. Tuttavia, questa metodologia risulta

discutibile e incoerente in quanto tali metriche riflettono solo indirettamente la percezione degli stakeholder. [91]

Pertanto, tra gli indicatori più appropriati vi è il Reputational Quotient (RQ), ovvero il quoziente reputazionale, ideato alla fine degli anni '90 da Charles Fombrun, professore e direttore del Reputational Institute a New York. L'RQ, poi evoluto nel modello RepTrak Pulse citato in precedenza, è un indice composto derivato da sondaggi presso stakeholder multipli, che misura la reputazione di un'azienda su sei dimensioni chiave:

I. Prodotti e servizi (qualità, valore, affidabilità),
II. Apprezzamento emotivo (quanto l'azienda è amata e rispettata),
III. Performance finanziaria (solidità economica percepita),
IV. Responsabilità sociale (impegno verso la comunità e l'ambiente),
V. Visione e leadership (chiarezza strategica e leadership efficace),
VI. Ambiente di lavoro (qualità della gestione e condizioni lavorative).

Ciascuna dimensione è valutata attraverso una serie di parametri specifici e concorre al punteggio reputazionale complessivo. [92] Di seguito lo schema che illustra le sei dimensioni e la scala numerica con cui si può misurare la reputazione.

[91] Fombrun, C. J., Gardberg, N. A., & Sever, J. M. (2000). The Reputation QuotientSM: A multi-stakeholder measure of corporate reputation. *The Journal of Brand Management, 7*(4), 241–255. https://doi.org/10.1057/bm.2000.10

[92] Özbağ, G. K., & Çekmecelioğlu, H. G. (2019). Examining the effects of dimensions of corporate reputation on firm performance. *The European Proceedings of Social & Behavioural Sciences (EpSBS)*, Joint Conference: 14th ISMC and 8th ICLTIBM-2018. https://doi.org/10.15405/epsbs.2019.01.02.24

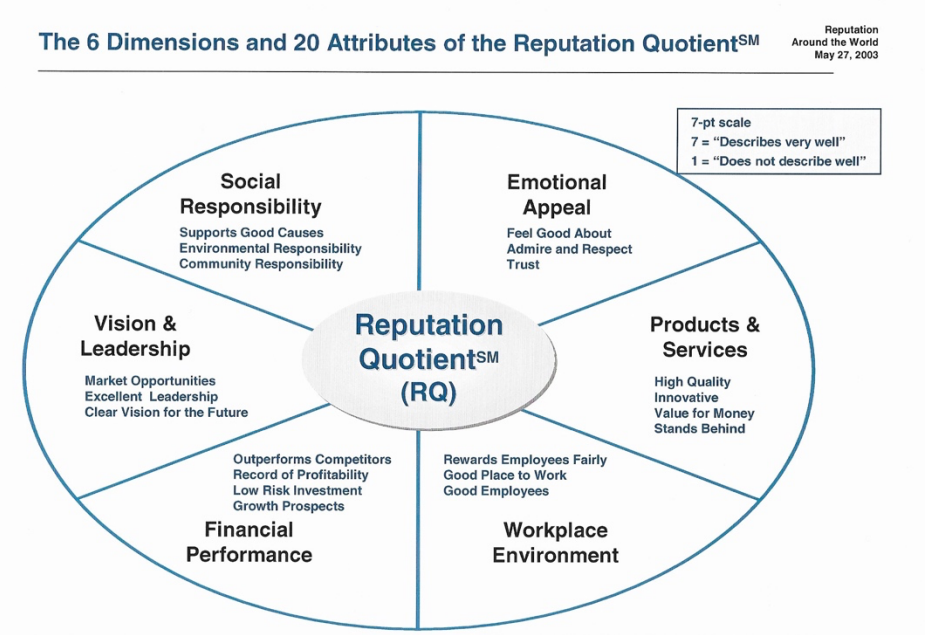



Figura 15: Struttura del Reputation Quotient: dimensioni e attributi chiave della reputazione aziendale. Fonte: Reputation Institute

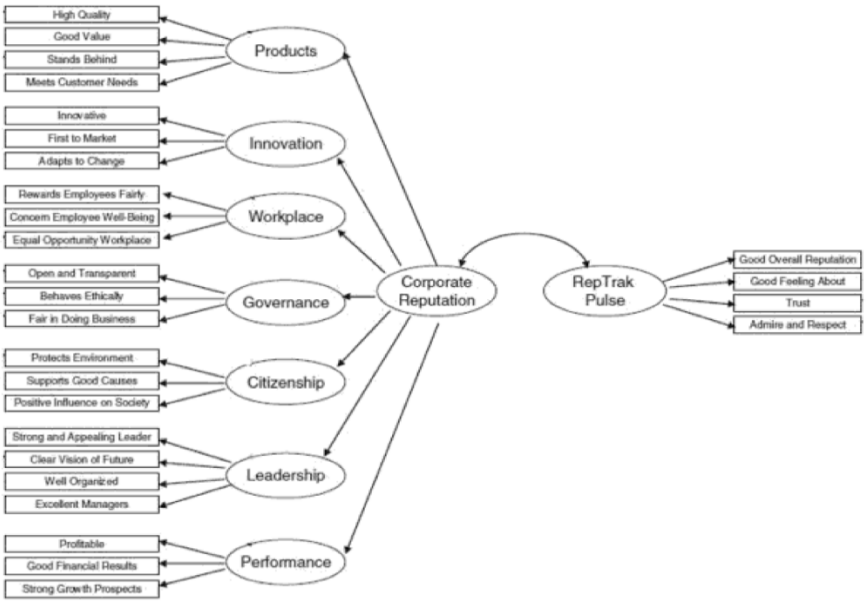
Tuttavia, questo modello venne testato e perfezionato nel corso degli anni, dando vita al Reputational Trak Pulse (RepTrak Pulse), introdotto nel 2005 dal Reputational Institute. Dal 2006 in poi, è stato utilizzato per misurare la reputazione delle aziende con il maggior fatturato a livello globale.

L'obiettivo degli autori era quello di creare uno strumento di analisi che fosse allo stesso tempo sintetico, intuitivo e facilmente integrabile con altri modelli esistenti. Il RepTrak Pulse permette infatti di analizzare come il pubblico e gli stakeholder percepiscono la reputazione di un'azienda, consentendo confronti tra diversi gruppi di stakeholder o tra realtà aziendali appartenenti a paesi e contesti culturali differenti.

I fondatori spiegano che questo modello è in grado di catturare la reputazione aziendale in forma compatta, ponendo particolare attenzione alla sua componente emotiva, considerata infatti il "cuore pulsante" dell'identità reputazionale. Il modello si basa su quattro indicatori legata all'attrattività emotiva: la fiducia, l'ammirazione, il rispetto e la percezione complessiva dell'azienda. Su questa base, il Reputational Institute valuta ogni anno la reputazione di circa 7.000 aziende in 50 paesi, intervistando circa 60.000

consumatori. Il punteggio reputazionale finale è dato dalla media dei voti ricevuti su quei quattro indicatori, raccolti tra tutti gli intervistati che conoscono l'azienda.
In seguito, il modello venne ulteriormente ampliato in sette dimensioni chiave, articolate in ventitré indicatori.
L'immagine sottostante illustra i parametri che vengono considerati:

**Figura 1.2 - Dimensioni e indicatori del modello RepTrak Pulse**




**Fonte: Fombrun, Ponzi e Newburry, 2015**

Figura 16: Le sette dimensioni del modello repTral Pulse e i relativi indicatori di reputazione. Fonte: Fombrun, Ponzi e Newburry (2015)

Per comprendere in modo concreto come viene valutata la reputazione di un'azienda utilizzando l'indice RepTrak, si può osservare in caso di Equifax e l'impatto immediato subìto dopo l'incidente. L'indice, che misura la reputazione attraverso diverse dimensioni (come performance, innovazione, governance e fiducia), evidenzia chiaramente il calo registrato tra febbraio e ottobre 2017.

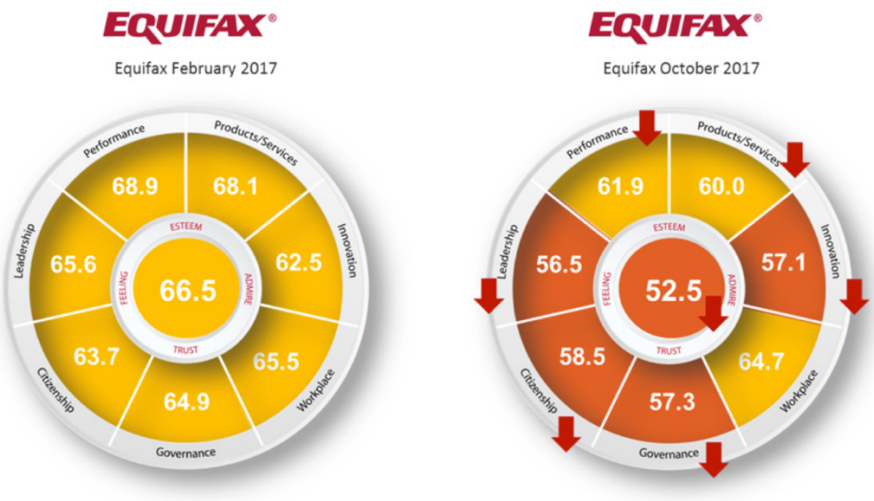



Figura 17: Reputazione di Equifax prima e dopo l'attacco informatico del 2017 (modello RepTrak). Fonte: Reputation Institute

Questo caso dimostra come un singolo evento possa influenzare negativamente la percezione pubblica e abbattere la reputazione aziendale misurata dal RepTrak. Proprio per questo, ogni anno viene pubblicata la classifica "Global RepTrak 100", che individua le 100 aziende con la migliore reputazione al mondo. [93]

Sul fronte del risk management, alcune società specializzate hanno elaborato altri indici sintetici di rischio reputazionale. Infatti, in aggiunta all'RQ e al RepTrak, la società RepRisk ha elaborato un Reputation Risk Index (RRI) che, tramite analisi dei media e fonti pubbliche in 20 lingue, quantifica un punteggio di rischio reputazionale legato a tematiche ESG e di condotta aziendale. Analogamente, agenzie come Moody's e S&P hanno iniziato a includere considerazioni di *reputational risk* nel rating qualitativo, specialmente per settori come quello finanziario dove la fiducia è essenziale.

In definitiva, nessun singolo indicatore o metrica di misurazione può cogliere pienamente la reputazione, ma solamente l'osservazione combinata di più parametri, tra cui azioni, clienti, sondaggi, indicatori ecc., forniscono un quadro abbastanza chiaro. Ma comunque rimane il fatto che la misurazione della reputazione aziendale è un tema complesso, difficile da gestire e mettere in atto.

[93] Corradini, F., & Nardelli, G. (2015). *La gestione della reputazione aziendale nell'era digitale*. FrancoAngeli.

### 2.5 Reputazione a livello Paese: cybersecurity, governance e percezione economica

Oltre ad influenzare la reputazione delle singole aziende, la dimensione della sicurezza informatica sta diventando un fattore rilevante anche per la reputazione economica di interi paesi. Pertanto, in un'economia sempre più interconnessa e digitale, Stati e governi vengono giudicati, da investitori, aziende e organizzazioni internazionali, anche in base alla loro affidabilità e resilienza sul fronte cyber. Dunque, si può parlare di "reputazione Paese" in ambito cybersecurity, intendendo come un paese sia percepito in termini di sicurezza degli ambienti digitali, efficacia nel contrastare le minacce e protezione delle infrastrutture critiche e dei dati.

Ma quali elementi contribuiscono alla reputazione cyber nazionale?

Innanzitutto, il primo aspetto è legato alla frequenza e gravità degli attacchi informatici subiti dal paese. Nazioni che appaiono spesso colpite da grandi *data breach* o da cyberattacchi a servizi essenziali rischiano di essere percepite come insicure o tecnologicamente arretrate in tema di difesa digitale, causando perdite economiche, danni alla reputazione del paese, interruzioni nei servizi e rischi per la sicurezza nazionale. Questo significa che quando uno Stato è colpito ripetutamente, la sua immagine e la sua credibilità risultano compromesse. Basti pensare al caso Colonial Pipeline, in cui un ransomware paralizzò gran parte della costa orientale degli Stati Uniti, sollevando dubbi sulla capacità di governance e sulla modernità e sicurezza delle difese. Esempio come questo dimostrano come un singolo attacco informatico possa avere ripercussioni significative, fino a configurarsi come una vera e propria emergenza nazionale. Altro caso noto ancora non citato, è legato alle agenzie di governo della Costa Rica che nel 2022 subirono un attacco ransomware talmente grave che costrinse il presidente a dichiarare lo stato di emergenza nazionale, impattando sulla sicurezza dell'intero paese.

Dunque, l'impatto che un attacco cyber può avere sulla reputazione di un paese può essere drastico e gravemente dannoso, ma è importante valutare come la nazione colpita risponde ed impara da essi.

Un secondo fattore è la qualità della governance e delle normative in materia di cybersecurity. Paesi che adottando leggi rigorose, standard elevati e investono in agenzie per la sicurezza cibernetica tendono a costruirsi una reputazione di affidabilità. Ad

esempio, l'UE con il Regolamento GDPR e la Direttiva NIS ha segnato un approccio serio alla sicurezza e privacy, rafforzando la fiducia nel mercato digitale europeo. Il World Economic Forum e l'ITU stilano periodicamente indici e report globali di cybersecurity, tra cui il Global Cybersecurity Outlook e il Global Cybersecurity Index, che tengono conto di misure legali, tecniche e organizzative adottate dai paesi. Le nazioni ai vertici di queste classifiche, spesso economicamente avanzate, utilizzano tali riconoscimenti per promuovere la propria immagine di "partner digitale sicuro". [94] Un caso interessante riguarda il Pakistan, che spesso non viene considerato come un paese in cima a questi ranking, ma nel Global Cybersecurity Index 2024 ha conquistato il livello più alto della graduatoria, accanto a nazioni come gli Stati Uniti, il Giappone, Australia, Arabia Saudita e Malesia. Questo riconoscimento sottolinea notevoli progressi compiuti dal paese nell'implementazione di misure robuste di cybersicurezza e nel rafforzamento della protezione di infrastrutture critiche. [95] Dunque, i progressi in cybersecurity possono tradursi in soft power e reputazione positiva da attribuire al paese.

Come terzo fattore, bisogna considerare il livello di sviluppo economico (PIL) dei paesi. Generalmente, le nazioni ad alto reddito dedicano più risorse alla sicurezza informatica, formando professionisti e implementando tecnologie avanzate, il che li aiuta a prevenire grossi incidenti, o almeno a contenerli. Questo crea un circolo virtuoso, in cui se l'economia è forte, crescono gli investimenti in cybersecurity, si registrano meno incidenti, la reputazione rimane alta e stabile e gli investimenti aumentano. Viceversa, nei paesi con governance debole e risorse limitate possono diventare bersagli frequenti o terreno fertile per i cybercriminali, in quanto aziende e cittadini non vengono adeguatamente protetti. Difatti, ciò può scoraggiare operatori esteri dall'entrare in un mercato debole per timore di subire perdite. Per esempio, se un paese in via di sviluppo registra attacchi continui alle proprie banche e infrastrutture senza riuscire a contrastarli, gli investitori potrebbero esitare a collocarvi investimenti strategici per timore di furti di

[94] International Telecommunication Union. (2024). *Global Cybersecurity Index (GCI): Measuring countries' commitment to cybersecurity across five pillars* [Report]. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[95] CSO Pakistan. (2024, 17 settembre). *ITU recognizes Pakistan's top-tier cybersecurity performance*. https://csopakistan.com/itu-recognizes-pakistans-top-tier-cybersecurity-performance/

informazioni e instabilità operativa, portando il territorio in questione ad avere ulteriori spese economiche da dover gestire.

Pertanto, risulta evidente che la reputazione di un paese in ambito cyber si riflette anche nella capacità di una nazione di essere vista come fornitrice di tecnologie sicure. Basti pensare al settore ICT, in cui territori dove i prodotti tecnologici sono considerati insicuri subiscono limitazioni, facendo sorgere dubbi a terzi. Un esempio è la Cina con Huawei: al di là delle motivazioni geopolitiche, le accuse di scarsa trasparenza e possibili backdoor nelle apparecchiature di alcuni server hanno influenzato la reputazione del paese come fornitore di high-tech, portando diversi stati occidentali a limitarne l'utilizzo nelle reti 5G per paure legate alla cybersecurity. [96] Allo stesso modo, nazioni note per essere un fulcro di cybercriminali e sponsor di attacchi (come la Corea del Nord o la Russia) subiscono una reputazione negativa che trascende l'ambito digitale, contribuendo all'isolamento economico. Di conseguenza, essere nella lista di paesi da cui provengono molti attacchi informatici, può danneggiare e minare la reputazione delle nazioni stesse, portando altri stati a considerare misure difensive o restrittive.

Altro elemento collegato alla reputazione nazionale è la capacità di perseguire e punire i criminali informatici sul proprio territorio. Ne consegue che, alcuni hacker possono sentirsi più sicuri ad operare in determinati paesi, in quanto non esistono leggi adeguate o volontà politica di fermarli, impattando sulla reputazione. In aggiunta, il territorio verrà percepito come rischioso per un'eventuale cooperazione economica e soprattutto poco collaborativo in un mondo sempre più interconnesso, in cui un attacco informatico in una determinata zona del mondo potrebbe propagarsi molto velocemente e indirettamente anche a molti chilometri di distanza.
Dunque, paesi che collaborano attivamente nelle operazioni di sicurezza informatica costruiscono un'immagine di attore affidabile e responsabile nel cyberspazio, contribuendo in modo proattivo a quel senso di responsabilità collettiva di cui si parlava nel Capitolo 1.

[96] Berman, N., Maizland, L., & Chatzky, A. (2023, 8 febbraio). *Is China's Huawei a Threat to U.S. National Security?*Council on Foreign Relations. https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security

In definitiva, analizzando questi fattori, si evince che la sicurezza informativa ormai è divenuta parte integrante della reputazione economica nazionale. Tradizionalmente la reputazione di un paese era associata a fattori come stabilità politica, rispetto della legge, infrastrutture fisiche e qualità del capitale umano. Ad oggi, a questi si aggiunge la percezione di stabilità e sicurezza digitale: un paese all'avanguardia nelle difese cyber, con basso tasso di crimine informatico sarà visto come un ambiente più sicuro per investimenti, soprattutto nel settore hi-tech; mentre, una nazione frequentemente colpita da cyber attacchi perde attrattività economica.

### 2.6 Cyber attacchi e attrattività economica: il legame con investimenti e fiducia nel sistema-paese

La correlazione discussa nel paragrafo precedente viene ormai riconosciuta nelle analisi sull'attrattività economica di un paese. In particolare, si osservano correlazioni e possibili nessi causali tra la frequenza/gravità degli attacchi informatici e parametri come i flussi di investimenti diretti esteri, la competitività nell'attrarre imprese high-tech e la fiducia degli investitori istituzionali.

In un mondo dove le imprese multinazionali devono scegliere dove allocare capitale, aprire sedi o stabilimenti produttivi, la valutazione del rischio paese si è allargata includendo componenti digitali. Per esempio, se un'azienda che deve aprire un nuovo data center regionale, non sarà rilevante solo il costo dell'energia o la stabilità politica della nazione ospitante, ma anche la robustezza dell'ecosistema cyber locale. Difatti, la presenza di professionisti qualificati in sicurezza, normative efficaci contro il cybercrimine, probabilità di subire interruzioni per attacchi sicuramente agevola l'investimento. Mentre, un paese con infrastrutture insicure potrebbe esporre l'impresa a costi maggiori di protezione o a rischi di fermo operativo. Dunque, scegliere un territorio con standard di sicurezza elevati e proteggere le infrastrutture critiche sta diventando un fattore reale nelle scelte di localizzazione. Questo suggerisce che territori percepiti come cyber insicuri potrebbero vedere opportunità di investimento sfumare a vantaggio di concorrenti più sicuri. [97]

[97] Kaspar, M. (2023, 6 novembre). *The rise of cybersecurity in location decisions*. fDi Intelligence. https://www.fdiintelligence.com/content/6f72b474-145e-5eef-9079-874a0ac2a59e

Sebbene non sia stato documentato un effetto preciso del Global Cybersecurity Index sul volume degli investimenti high tech ricevuti da un paese, studi di Oxford Economics evidenziano come una solida postura di sicurezza informatica favorisca l'innovazione e la fiducia nella trasformazione digitale. [98] Allo stesso modo, indagini recenti confermano che per molti investitori, dal settore pubblico a quello finanziario, i rischi cyber rappresentano una priorità strategica che influenza le valutazioni dei paesi e le scelte di investimento.

Un altro aspetto cruciale è la fiducia dei mercati finanziari globale. Gli investitori internazionali, come banche e fondi, valutano il rischio di investire in titoli di un certo paese. Se questo subisce un attacco devastante che paralizza, per esempio, il suo sistema finanziario per giorni, la percezione del rischio sale e potrebbe riflettersi in premi per il rischio maggiorati con tassi di interesse più alti e assicurazioni in rialzo. In sostanza la vulnerabilità cyber può tradursi in un costo paese. Viceversa, nazioni con reputazione di eccellenza cyber, come spiegato precedentemente, possono attrarre investimenti in settori avanzati perché gli investitori si sentono più sicuri sul fronte di protezione internazionale e continuità operativa. Oltre al tema legato agli investimenti, un'ulteriore dimensione più "interna" da considerare è relativa ai talenti e alla fuga di cervelli. Spesso professionisti ICT potrebbero essere più propensi ad andare a lavorare in paesi all'avanguardia e con infrastrutture digitali più forti e sicure, lasciando il proprio paese con meno capitale umano qualificato e dunque più rischioso in ambito cyber. Come si è visto nel paragrafo 2.6.5, il numero di professionisti non è distribuito in maniera omogenea, ma è concentrato principalmente in aree geografiche più avanzate, sia per una questione di opportunità lavorative, sia per una questione di opportunità accademiche.

Quanto analizzato fino ad ora, conduce ad un punto centrale: la frequenza e gravità degli attacchi in un paese possono essere viste come proxy della qualità dell'ambiente di cybersecurity di quel territorio. Se si osserva che in una nazione si verificano di continuo gravi attacchi, questo segnala problemi sistemici, come la carenza di misure di sicurezza,

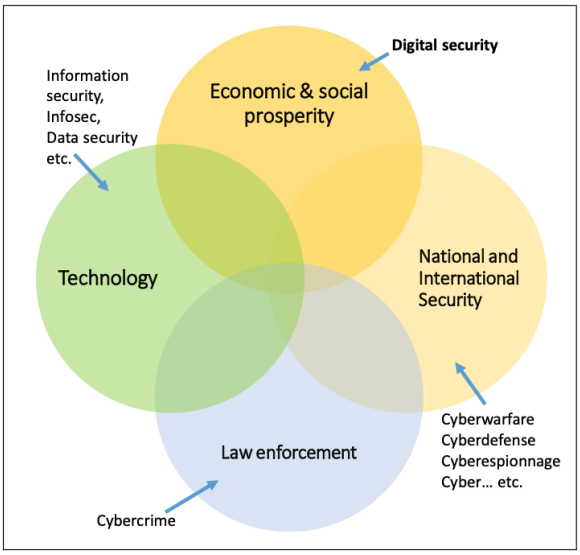
[98] Cisco & Oxford Economics. (2016, maggio). *Cybersecurity as a Growth Advantage*.https://www.oxfordeconomics.com/resource/cybersecurity-as-a-growth-advantage/

lacune normative e poca consapevolezza delle conseguenze. Questo sintomo negativo, dunque, potrà influire sul rating, sulle decisioni di investimento e sulla fiducia generale. Di conseguenza, rapporti come il Global Risk Report del WEF hanno iniziato a includere la cyber resilienza tra i fattori rischio-paese discussi, e organizzazioni come Standard & Poor's valutano di incorporare un Cyber Risk Index nelle pagelle sovrane. L'OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico) ha pubblicato un policy framework in cui esorta i governi ad agire sul tema della cybersecurity e sostenere l'attività economica e l'innovazione digitale, riconoscendo in modo implicito che la fiducia negli ecosistemi digitali è una condizione necessaria per la crescita.

La Figura 18, elaborata nel framework di cui sopra, aiuta a comprendere visivamente quanto discusso nel paragrafo. La sicurezza digitale non è confinata a un ambito puramente tecnico, ma rappresenta un fattore trasversale che tocca la prosperità economica e sociale, la sicurezza nazionale e internazionale e la capacità di contrasto alla criminalità. In questo senso, la rappresentazione OCSE dimostra bene che la cybersecurity è ovunque: costituisce la base per la continuità operativa delle imprese, influenza le scelte di localizzazione degli investimenti e contribuisce a rafforzare la fiducia complessiva nel sistema-paese. [99]

[99] OECD. (2022). *OECD Policy Framework on Digital Security: Cybersecurity for Prosperity* [Report]. OECD Publishing. https://doi.org/10.1787/a69df866-en

Figure 2. Digital security, the economic and social aspect of cybersecurity




Source: OECD

Figura 18: La cybersicurezza come intersezione tra tecnologia, prosperità economico-sociale, sicurezza nazionale e law enforcement. Fonte: OECD

Tuttavia, non bisogna generalizzare: la relazione tra attacchi informatici e attrattività economica non è automatica. Infatti, i paesi più avanzati e competitivi sul piano globale, come gli Stati Uniti, sono spesso anche i più colpiti dagli attacchi, ma questo non li rende meno attrattivi. Al contrario, la loro forza risiede nella capacità di investire tanto in difese e reagire con decisione. Un caso significativo è rappresentato da SolarWinds, dopo il quale gli USA hanno introdotto sanzioni e nuove norme per rafforzare la sicurezza della catena di fornitura. In quest'ottica, ciò che conta non è soltanto la frequenza degli attacchi, ma il loro tasso di successo e, soprattutto, la risposta istituzionale che ne consegue.

## Conclusioni Capitolo 2

I temi trattati in questo capitolo hanno messo in luce come la reputazione, sia aziendale che nazionale, risenta fortemente della dimensione cyber. Per cominciare è stata fatta una panoramica sul tema della reputazione a livello aziendale, seguita da esempi rappresentativi in contesti e settori diversi. Infine, è stato approfondito il tema reputazionale in ambito di sistema-paese per poter procedere con un'ulteriore analisi empirica.

## CAPITOLO 3 – METODOLOGIA E ANALISI EMPIRICA

Alla luce di tali premesse teoriche, il Capitolo 3 intende tradurre queste riflessioni teoriche in un'analisi empirica, con l'obiettivo di verificare se e in che misura la frequenza degli attacchi informatici possa essere messa in relazione con indicatori socioeconomici come il PIL di un paese, la classe di redditività, il numero di utenti presenti su Internet e la popolazione di una nazione utilizzato il software SPSS. Questo approccio permette di osservare non soltanto le differenze tra settori economici, ma anche le dinamiche a livello nazionale, facendo emergere come le variabili economiche e digitali possono incidere sulla vulnerabilità di un paese.

### 3.1 Dataset e preparazione dei dati

Il dataset impiegato per questa analisi proviene dal Cyber Events Database del Center for International and Security Studies at Maryland (CISSM). Pur essendo limitato ai soli attacchi resi pubblici e quindi a informazioni frammentarie, raccoglie dati disponibili su attacchi informatici avvenuti a livello globale dal 2014 al gennaio del 2025. Il campione contiene in totale 14.652 osservazioni in totale.

Ogni record del database rappresenta un singolo incidente e include informazioni quali: la data dell'evento, l'organizzazione vittima, il paese bersaglio, il settore economico colpito, la tipologia di attacco, il movente e, se noto, l'attore responsabile ecc. Ai fini di questa analisi, le variabili di interesse estratte sono:

- il paese vittima dell'attacco,
- il settore dell'organizzazione colpita,
- l'anno dell'evento (dal 2014 al 2024)

Inoltre, per una breve analisi descrittiva verranno considerate anche le variabili relative al motivo dell'attacco e il paese attaccante.

Dopodiché, dal World Bank Group sono stati scaricati i seguenti dataset:

- file contenete valori del PIL (in USD correnti) relativi ad ogni paese dal 2014 al 2024, incorporati sotto la variabile PIL (mln);
- informazioni relative alla classificazione dei paesi in base alle classi di redditività "High income", "Upper middle income" e "Lower middle income", nel periodo

2014-2024. Tali categorie sono state registrate sotto la variabile Classe di Reddito WB con l'obiettivo di consentire analisi comparative e approfondimenti nelle fasi successive della ricerca;

- dati relativi alla popolazione di ciascun paese di interesse dal 2014 al 2024 (variabile Popolazione);
- percentuale di utenti che utilizzano Internet sempre nella fascia temporale presa in analisi (variabile Numeri utenti su Internet % della popolazione). Per trasformare questi ultimi valori in numeri, è stata creata un'ulteriore variabile che tiene presente del numero effettivo di utenti che utilizzato Internet in ciascun paese (Utenti Internet mln).

Una volta aggregati tutti i dati, il dataset completo contiene le seguenti variabili:

- Anno
- Settore
- Motivo
- Paese
- Paese Attore
- PIL (US$) mld
- Numeri Utenti su Internet (% della popolazione)
- Popolazione (mln)
- Classe di Reddito WB
- Utenti Internet (mln)

Ai fini delle analisi successive, sono stati calcolati i parametri elencati di seguito:

- LogPIL
- LogNumeriUtentiSuInternet

Queste modifiche sono state effettuate per ridurre il bias dovuto alla dimensione demografica dei paesi riducendo le distorsioni di valori estremi, per migliorare la comparabilità tra paesi con diversa scala economica e ridurre l'impatto delle forti asimmetrie distributive.

Prima di andare ad operare sul software SPSS, si è fatta una pulizia dei dati a disposizione. Tramite l'utilizzo della tabella Pivot su Excel, sono emersi molti errori ed osservazioni poco significative. Le correzioni fatte sono state le seguenti:

- sono stati esclusi dall'analisi paesi con un numero totale di attacchi inferiore a 50, poiché ritenuti poco significativi e potenziali outlier che potrebbero minare la stabilità statistica delle stime;
- le voci "Undetermined" presenti nelle variabili Paese e Settore sono state scartate in quanto non utilizzabili nell'analisi;
- per poter integrare le informazioni provenienti dal World Bank Group e rendere il dataset finale uniforme, sono state ricodificate delle voci in merito alla battitura dei nomi di nazioni ed aggiunti dati mancanti riguardo al PIL della Korea (the Republic of) nel 2024.[100]
- infine, ai fini dell'analisi, sono state scartate le osservazioni relative agli attacchi registrati nel gennaio 2025.

Dunque, le nazioni che sono state escluse sono 132 e sono raffigurare nella mappa sottostante:

[100] IMF. (2024, 10 ottobre). South Korea: Gross domestic product (GDP) in current prices from 1987 to 2029 (in billion U.S. dollars). Statista. https://www.statista.com/statistics/263579/gross-domestic-product-gdp-in-south-korea/

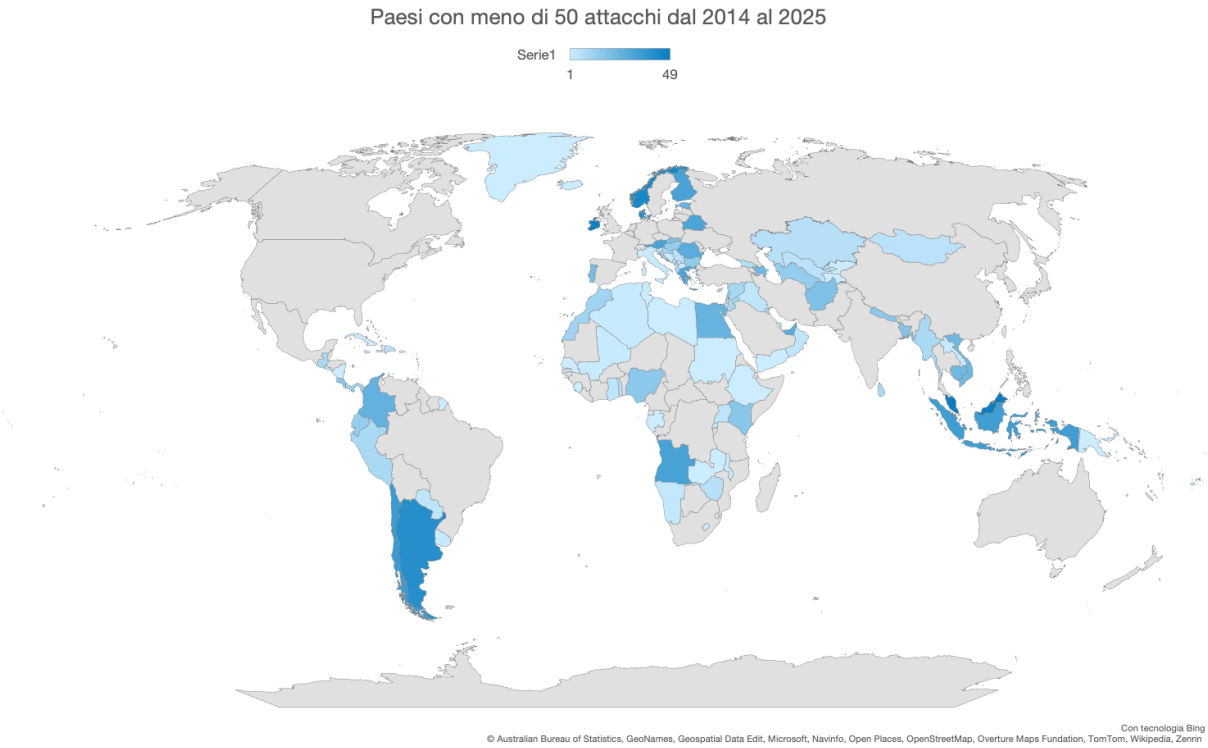



Figura 19: Numero di attacchi informatici dal 2014 al 2024. Fonte: eventi registrati nel CISSM.

Come si può osservare, la distribuzione geografica evidenzia come tali nazioni siano concentrate soprattutto in Africa, in alcune aree del Medio Oriente e l'Asia centrale, nonché in diversi stati del Sud America. In generale, si tratta di paesi con un livello di digitalizzazione più limitato o con una minore trasparenza della pubblicazione dei dati relativi agli incidenti di cybersicurezza. Se ci si concentra sull'Europa, si nota che diversi paesi presentano un numero di attacchi poco significativo. Si tratta in particolare di stati dell'Europa orientale e balcanica, ma anche di alcuni paesi di dimensioni ridotte. Questa distribuzione suggerisce che, rispetto alle grandi economie europee più digitalizzate, i paesi con minore esposizione internazionale o con una limitata capacità di reporting tendono a registrare un numero inferiore di incidenti informatici resi pubblici. Da precisare che l'Italia è presente nella mappa, poiché sono stati registrati due attacchi nello dello Stato del Vaticano.

Scartati questi dati, il nuovo campione, contiene 13.129 osservazioni e in totale 35 paesi inclusi nella ricerca, raffigurati nella seguente figura:

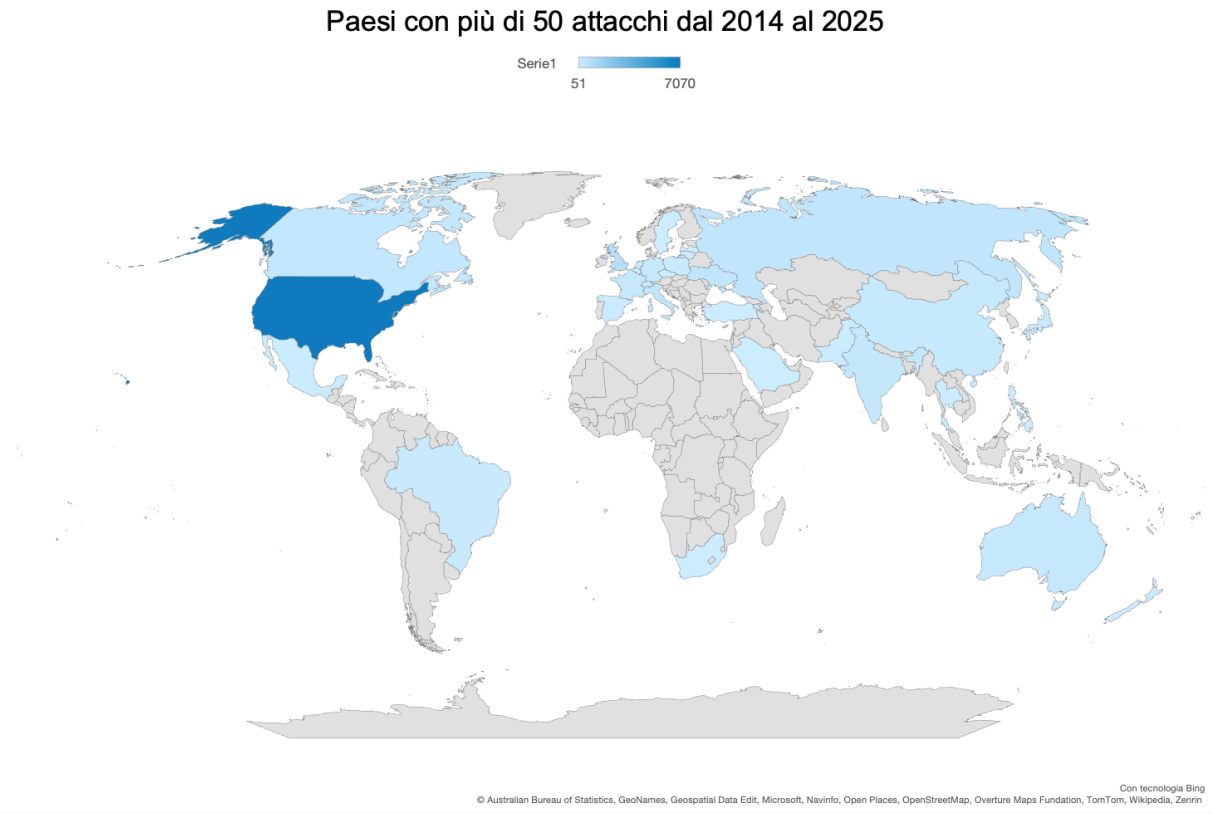



Figura 20: Numero di attacchi informatici dal 2014 al 2024. Fonte: eventi registrati nel CISSM.

Come emerge dalla Figura 20, gli attacchi sono concentrati prevalentemente in Nord America, e in misura minore, in alcune aree dell'Asia e dell'Europa. Questo suggerisce che gli episodi di cyberattacco sono legati soprattutto a paesi con un'elevata esposizione digitale e infrastrutture critiche diffuse.

Per avere una visione più ampia e completa del fenomeno e dei dati presenti nel file, le variabili relative al movente e al paese mandante sono state rappresentate nei grafici sottostanti.

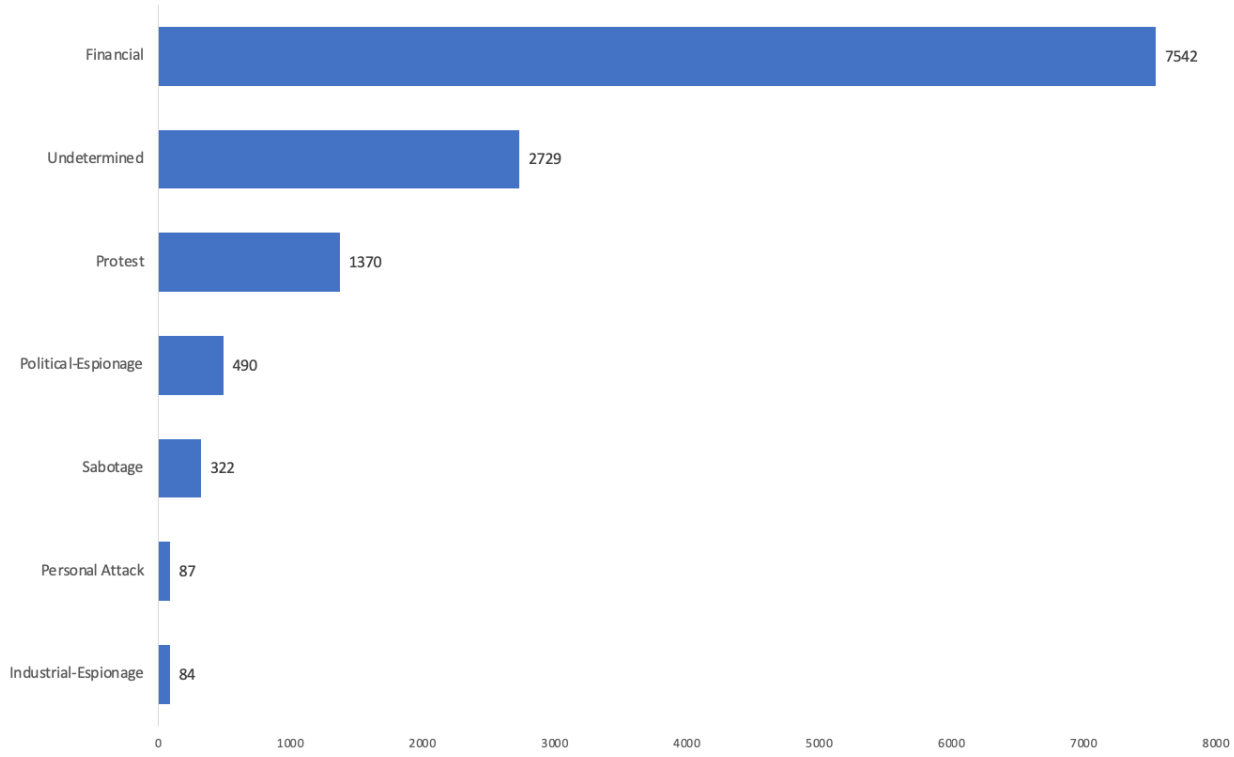



Figura 21: Conteggio delle motivazioni dietro ad un attacco informatico. Fonte: eventi registrati nel CISSM.

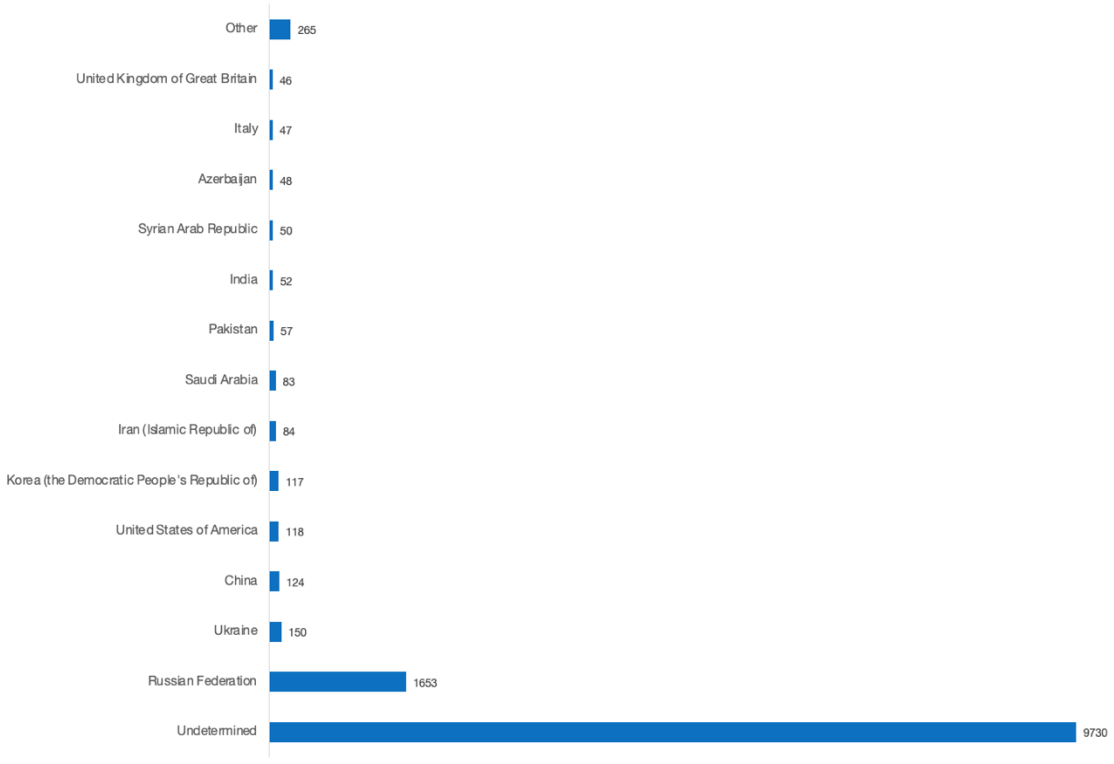



Figura 22: Conteggio dei paesi attori degli attacchi informatici. Fonte: eventi registrati nel CISSM.

Nelle precedenti figure sono riportati rispettivamente il conteggio delle motivazioni alla base di un attacco informatico e il numero di attacchi per paese di origine. Dalla Figura 21 emerge chiaramente che la principale motivazione degli attacchi informatici è di natura finanziaria, a conferma di quanto discusso nei capitoli teorici. Infatti, il cyberspazio rappresenta ormai un canale privilegiato per attività criminali finalizzate all'ottenimento di guadagni economici rapidi e difficilmente tracciabili. Accanto a questa finalità prevalente, si distinguono altre due categorie di motivazioni particolarmente rilevanti: gli attacchi condotti per protesta (es. gruppi hacktivisti) e quelli finalizzati allo spionaggio politico. In tutti e due i contesti, la dimensione reputazione diventa centrale, in quanto, nel primo caso l'attacco informatico viene utilizzato come strumento di pressione simbolica e mediatica; mentre, nel secondo caso come mezzo per erodere la fiducia nei confronti delle istituzioni e minare la percezione di stabilità di un paese.

Invece, la Figura 22 mostra la distribuzione dei principali paesi identificati come origine degli attacchi cyber. Il dato più rilevante riguarda la categoria "Undetermined", che con 9.730 casi rappresenta la quota largamente predominante. Questo risultato evidenzia come, nella maggior parte degli episodi, non sia possibile attribuire con certezza la responsabilità a un determinato paese, a causa sia delle difficoltà tecniche di tracciamento sia delle strategie di offuscamento adottate dagli attaccanti.
Tra i paesi effettivamente indicati, la Federazione Russa occupa la posizione più significativa, con 1.653 attacchi attribuiti, a conferma del ruolo centrale che questo attore riveste nel panorama della cybersicurezza internazionale. Tale evidenza è coerente con le analisi presenti in letteratura, che sottolineano la frequente attribuzione di attacchi alla Russia in ragione sia delle sue capacità offensive consolidate, sia del contesto geopolitico. Inoltre, un altro aspetto rilevante da osservare relativo alla Figura 22, in cui compaiono alcuni paesi che non erano stati inclusi nella variabile Paese come destinatari di attacchi informatici, poiché il numero di casi risultava non significativo. Tuttavia, tali nazioni emergono nella lista degli attori di attacchi cyber. Tra questi è interessante notare la Korea (the Democratic People's Republic of), che registra 117 attacchi lanciati a fronte di soli 3 attacchi subiti nell'arco di dieci anni. Questo divario può essere interpretato come il risultato di un livello relativamente contenuto di esposizione digitale interna, tipico di un regime fortemente controllato e poco aperto alla connettività globale, che riduce le

vulnerabilità a intrusioni esterne, contrapposta a una significativa attività offensiva rivolta verso l'esterno.

Dopo aver presentato una panoramica delle informazioni contenute nel dataset e averle ricondotte agli aspetti teorici discussi nei capitoli precedenti, si può procedere con l'analisi statistica delle variabili considerate.

## 3.2 Domanda di ricerca e formulazione ipotesi

L'obiettivo della ricerca è esaminare la relazione tra la frequenza degli attacchi informatici e il contesto economico dei paesi, misurato tramite il PIL e le classi di reddito delle nazioni, e valutare in che misura gli attacchi possano riflettere un rischio reputazionale a livello settoriale e nazionale in base all'esposizione digitale e alla popolazione della nazione. A tal fine, vengono impiegati degli strumenti statistici per testare quanto descritto nella letteratura, analizzando le tre ipotesi formulate per poter rispondere alla domanda di ricerca.
Le ipotesi sono:

H1: I paesi con fascia di reddito più alta registrano un numero maggiore di attacchi informatici.
H2: La frequenza degli attacchi varia significativamente tra settori nel corso degli anni.
H3: Il numero di attacchi eventi cyber influenza negativamente la performance economica di un paese, con possibili effetti sul PIL.

## 3.3 Metodologia

### 3.3.1 Esiste una differenza significativa nel numero di attacchi informatici in base alla fascia di reddittività del paese?

Per poter vedere se esiste una differenza significativa, i dati originari a livello di singolo attacco informatico sono stati aggregati in formato pannello Paese x Anno, così da avere come unità di osservazione la coppia (paese, anno). Questa scelta consente di confrontare i fenomeni tra le nazioni e lungo la dimensione temporale, evitando che i risultati siano

influenzati dalla diversa numerosità di eventi per singolo paese. In aggiunta alle variabili dei conteggi assoluti già presenti anche del dataset precedente, per ridurre il bias dovuto alla diversa dimensione demografica dei paesi e garantire un confronto più bilanciato del livello di esposizione, è stato calcolato un indicatore logaritmico riferito al numero di utenti su Internet. In questo caso, la variabile relativa al numero di attacchi si riferisce al numero di eventi cyber in un paese in un determinato anno.
Dunque, le variabili presenti nel nuovo dataset con variabili aggregate sono le seguenti:

- Paese
- Anno
- Numero di Attacchi
- Classe di Reddito WB
- PIL (US$) mld
- Numeri utenti su Internet (% della popolazione)
- LogPIL
- Popolazione (mln)
- Utenti Internet (mln)
- LogNumeriUtentiSuInternet

Le ipotesi che si sono andate a testare sono:
H0: le classi di reddito sono tutte uguali in termini di attacchi cyber
H1: almeno una è diversa

Per poter svolgere questa analisi, verrà utilizzato un modello lineare generalizzato, in quanto permette di fare regressioni adatte a dati non normali (in questo caso il conteggio di attacchi informatici). A causa dell'eccessiva varianza, come distribuzione per la variabile dipendente è stata selezionata la binomiale negativa, e come funzione la link log. Più nello specifico, come predittore è stata utilizzata la variabile categoriale Classe di Reddito WB come fattore e come variabile offset LogUtentiInternet. Lo scopo dell'analisi è quello di considerare il numero di attacchi in ogni anno in un determinato paese in rapporto alla popolazione esposta.

I risultati ottenuti sono i seguenti:

**Test degli effetti del modello**

| Origine | Tipo III Chi-quadrato di Wald | df | Sign. |
|---|---|---|---|
| (Intercetta) | 104,679 | 1 | <,001 |
| Classe di Reddito WB | 179,585 | 2 | <,001 |

variabile dipendente: Numero di Attacchi
Modello: (Intercetta), Classe di Reddito WB, offset = Log (UtentiInternet)

Figura 23: Test degli effetti del modello. Fonte: eventi registrati nel CISSM.

Dalla Figura 23 si evince che almeno una delle classi di reddito è diversa dalle altre. Più nel dettaglio, il p<0,001 indica che la fascia di reddito ha un effetto significativo sulla popolazione presente su Internet. Dunque, si rigetta l'ipotesi nulla e si può constatare che le differenze tra classi di reddito sono reali e molto forti.

Per capire quale delle categorie è più alta si osserva la seguente tabella:

**Stime dei parametri**

| Parametro | P | Errore std. | 95% intervallo di confidenza di Wald Inferiore | Superiore | Test sull'ipotesi Chi-quadrato di Wald | df | Sign. |
|---|---|---|---|---|---|---|---|
| (Intercetta) | -2,066 | ,1314 | -2,324 | -1,809 | 247,320 | 1 | <,001 |
| [Classe di Reddito WB=High-income ] | 1,982 | ,1489 | 1,690 | 2,274 | 177,107 | 1 | <,001 |
| [Classe di Reddito WB=Lower-middle-income] | 1,839 | ,2215 | 1,405 | 2,273 | 68,971 | 1 | <,001 |
| [Classe di Reddito WB=Upper-middle-income] | 0[a] | . | . | . | . | . | . |
| (Scala) | 1[b] | | | | | | |
| (Binomiale negativa) | 1[b] | | | | | | |

variabile dipendente: Numero di Attacchi
Modello: (Intercetta), Classe di Reddito WB, offset = Log(UtentiInternet)

a. Impostato su zero in quanto tale parametro è ridondante.

b. Fissata al valore visualizzato.

Figura 24: Stime dei parametri. Fonte: eventi registrati nel CISSM.

La colonna P è espressa in scala logaritmica, dunque, per poter trasformare i risultati in numeri naturali bisogna calcolare l'esponenziale ottenendo rispettivamente 7,3 e 6,3. Ne consegue che, i paesi ad alto reddito mostrano un tasso di attacchi circa 7,3 volte superiore rispetto ai paesi a reddito medio-alto (categoria di riferimento della variabile categoriale Classe di Reddito WB). Allo stesso modo, anche i paesi con reddito medio-basso risultano significativamente più esposti, con un tasso di attacchi pari a circa 6,3 quello dei paesi a reddito medio-alto. Questi risultati indicando che l'incidenza degli attacchi cyber non cresce linearmente con la ricchezza. Pertanto, le nazioni con reddito medio-alto appaiono

relativamente meno colpite, mentre quelle con reddito più alto e medio-basso registrano un numero significativamente maggiore di attacchi informatici per unità di popolazione connessa a Internet.

In definitiva, come evidenziato dei capitoli teorici, i paesi ad alto reddito tendono ad essere più vulnerabili e vittime di attacchi cyber. Le motivazioni sono relative alla maggior quantità di risorse economiche, tecnologiche e informative che questi stati detengono, le quali rappresentano obiettivi particolarmente appetibili per gli attaccanti. In aggiunta, la vasta digitalizzazione delle infrastrutture critiche, dei servizi finanziari e delle comunicazioni aumenta la superficie di attacco, e di conseguenza, la probabilità di subire intrusioni. A questo si aggiunge il fatto che le economie avanzate sono maggiormente interconnesse a livello globale, rendendo gli attacchi non solo più frequenti, ma anche più sofisticati e impattanti in termini economici e geopolitici.

### 3.3.2 La frequenza degli attacchi varia significativamente tra settori e negli anni?

Per poter osservare la frequenza di attacchi nei diversi settori, e riprendere quanto detto nei capitoli teorici, a livello visivo aiuta la creazione di un grafico a barre come il seguente:

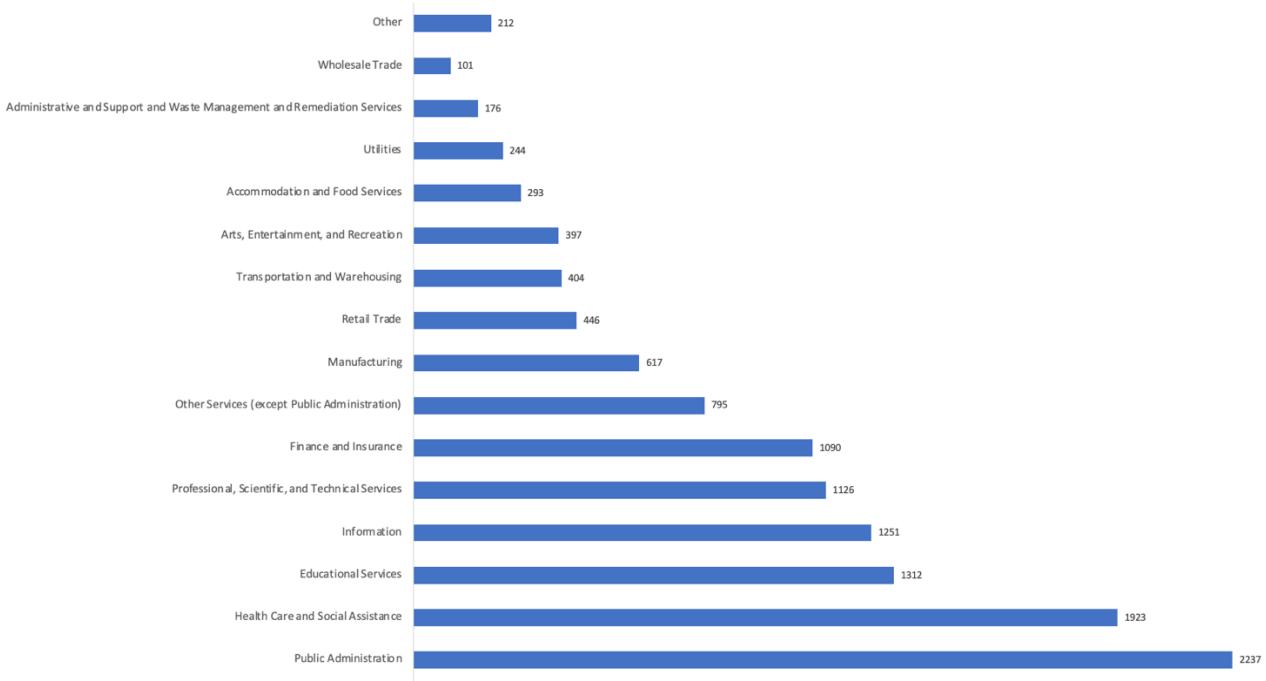



Figura 25: Conteggio attacchi informatici totali nei diversi settori. Fonte: eventi registrati nel CISSM.

Osservando la Figura 25, si può constatare che la distribuzione degli attacchi informatici tra i settori non è uniforme; pertanto, si è approfondita l'analisi concentrandosi su come sono distribuiti gli attacchi informatici nei diversi settori e nei diversi paesi. L'obiettivo è vedere se la distribuzione degli attacchi settoriali è uguale in tutti i paesi, oppure se alcuni paesi sono più bersagliati di altri. Per fare ciò, si è creata una tabella di contingenza, in cui sono state selezionare le variabili Settore come riga e Paese come colonna, ed è stato applicato il test di Monte Carlo, in quanto, facendo girare il test su 10.000 simulazioni causali, produce un p-value più affidabile e preciso anche in presenza di celle con valori molto piccoli. I risultati hanno mostrato che la distribuzione degli attacchi varia in modo significativo in funzione del settore e del paese (p<0,001).

**Test del chi-quadrato**

| | | | | Sign. Monte Carlo (bilaterale) | | |
|---|---|---|---|---|---|---|
| | | | | | Intervallo di confidenza 99% | |
| | Valore | df | Significatività asintotica (bilaterale) | Significatività | Limite inferiore | Limite superiore |
| Chi-quadrato di Pearson | 1365449,01[a] | 595 | <,001 | <,001[b] | <,001 | <,001 |
| Rapporto di verosimiglianza | 140244,177 | 595 | <,001 | <,001[b] | <,001 | <,001 |
| Test esatto di Fisher-Freeman-Halton | 142349,931 | | | <,001[b] | <,001 | <,001 |
| N di casi validi | 1048382 | | | | | |

a. 589 celle (90,9%) hanno un conteggio previsto inferiore a 5. Il conteggio previsto minimo è ,00.

b. Basato su 10000 tabelle campionate con seme iniziale 2000000.

Figura 26: Test del chi-quadro con simulazione di Monte Carlo Settore x Paese. Fonte: eventi registrati nel CISSM.

Inoltre, per capire quali celle contribuiscono maggiormente al risultato complessivo, sono stati calcolati i residui standardizzati.

Dallo studio della tabella di contingenza, emerge chiaramente che gli Stati Uniti rappresentano il paese con il maggior numero di attacchi informatici riportati. Tuttavia, questo risultato deve essere interpretato alla luce di un possibile bias del dataset, in quanto, trattandosi del database CISS sviluppato negli USA, è plausibile che i dati nazionali vengano raccolti e classificati con maggiore sistematicità rispetto ad altri paesi. Tale aspetto verrà poi discusso nel paragrafo dedicato alle limitazioni della ricerca.

Più nel dettaglio, accanto agli Stati Uniti, diverse nazioni mostrano residui standardizzati positivi e significativi in più settore, confermando la loro esposizione elevata: Di seguito un breve schemaa riassuntivo:

- Il Regno Unito, Canada e Australia, compaino ripetutamente in settori ad alta intensità di dati, come la pubblica amministrazione, l'istruzione, il settore finanziario e dei servizi professionali. Questo andameneto conferma sia il livello di digitalizzazione avanzata, sia l'integrazione nelle reti economiche e politiche occidentali.
- La Russia si distingue in particolare per gli attacchi cyber nel contesto finanziario e informativo, probabilmente collegato al contesto geopolitico e alla centralità del paese in operazioni di cyber warfare.
- L'Italia e la Germania, invece, registrano valori rilevanti nella pubblica amministrazione e nella manifattura, due settori particolarmente strategici per l'economia e dunque molto esposti.
- Mentre, la Cina e l'India, che rappresentano le due economie emergenti, mostrano concentrazioni elevate soprattutto nell'ambito dell'istruzione, della sanità e della manifattura, settori dove la rapida crescita della digitalizzazione si accompagna a vulnerabilità infrastrutturali.
- Infine, Israele, Ucraina e Russia presentano valori anomali del settore dell'infomazione e della pubblica amministrazione, coerentemente con il contesto geopolitico caratterizzato da conflitti e instabilità.

Per estendere ulteriormente l'analisi e analizzare l'evoluzione temporale degli attacchi, è stata costruita una tabella di contingenza Anno x Settore, valutata tramite il test del Chi-quadro con correzione Monte Carlo (sempre a causa della presenza di celle vuote). I risultati confermano un'associazione statisticamente significativa tra anno e settore ($p<0,001$), indicando che la distribuzione degli attacchi non è causale ma varia in maniera sistematica nel tempo.

**Test del chi-quadrato**

| | Valore | df | Significatività asintotica (bilaterale) | Sign. Monte Carlo (bilaterale) Significatività | Intervallo di confidenza 99% Limite inferiore | Intervallo di confidenza 99% Limite superiore |
|---|---|---|---|---|---|---|
| Chi-quadrato di Pearson | 1228106,36[a] | 187 | <,001 | <,001[b] | <,001 | <,001 |
| Rapporto di verosimiglianza | 138813,763 | 187 | <,001 | <,001[b] | <,001 | <,001 |
| Test esatto di Fisher-Freeman-Halton | 139380,387 | | | <,001[b] | <,001 | <,001 |
| N di casi validi | 1048382 | | | | | |

a. 188 celle (87,0%) hanno un conteggio previsto inferiore a 5. Il conteggio previsto minimo è ,00.

b. Basato su 10000 tabelle campionate con seme iniziale 1314643744.

Figura 27: Test del chi-quadro con simulazione di Monte Carlo Settore x Anno. Fonte: eventi registrati nel CISSM.

Dall'analisi dei residui emerge che nei primi anni (2014-2018), gli attacchi cyber erano relativamente più distribuiti tra i diversi comparti, sebbene già si notassero concentrazione nel settore manifatturiero e del commercio al dettaglio. Invece, a partire dal 2019 si osserva una netta riconfigurazione che vede concentrarsi gli attacchi in ambiti ad alta criticità come la sanità, la pubblica amministrazione, l'informazione e i servizi professionali, scientifici e tecnici. Mentre, dal 2020 si nota una crescita improvvisa e significativa di eventi nei comparti più strategici e critici, riconducibile a fattori esogeni quali la pandemia da Covid-19 e la conseguente diffusione del lavoro da remoto, maggiore digitalizzazione dei servizi e dunque, maggiore interconnessione a livello globale. Ulteriore conferma viene data dalla visualizzazione del seguente grafico:

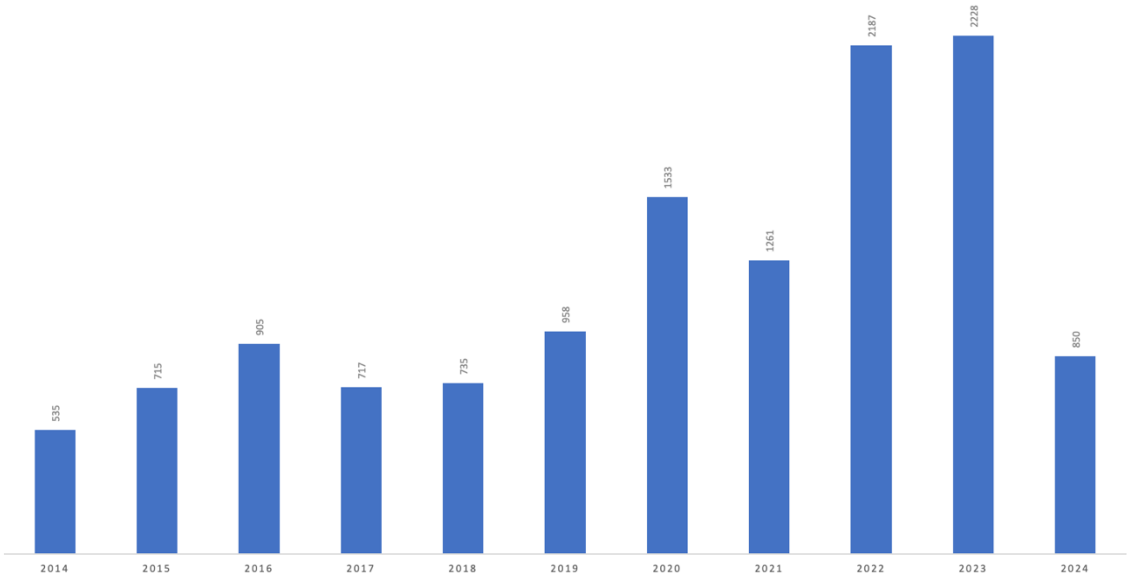



Figura 28: Conteggio annuale degli attacchi informatici (2014-2024). Fonte: eventi registrati nel CISSM.

Per poter entrare ancora più nel dettaglio e formalizzare la dinamica temporale degli attacchi, è stato stimato un modello di regressione di conteggio (Binomiale negativa a causa dell'elevata varianza), con Numero di Attacchi come variabile dipendente e Anno, Settore e Paese come effetti fissi. Prima di fare ciò, è stato creato un nuovo dataset con variabili aggregate: Anno x Paese x Settore.

Una volta svolta l'analisi, i risultati indicano che tutti e tre i fattori incidono in modo significativo sul numero di attacchi cyber ($p<0,001$).

**Test degli effetti del modello**

| Origine | Tipo III Chi-quadrato di Wald | df | Sign. |
|---|---|---|---|
| (Intercetta) | 57,164 | 1 | <,001 |
| Anno | 80,952 | 10 | <,001 |
| Settore | 243,843 | 16 | <,001 |
| Paese | 1262,906 | 34 | <,001 |

Variabile dipendente: Numero_Attacchi
Modello: (Intercetta), Anno, Settore, Paese

Figura 29: Stima del modello di regressione binomiale negativa. Fonte: eventi registrati nel CISSM.

Analizzando la tabella delle Stime dei Parametri, a partire dal 2020 si osserva un incremento statisticamente significativo (ad esempio, nel 2022 e 2023 il $p<0,001$), coerente con quanto affermato nel paragrafo precedente e con eventi esogeni come la pandemia e successivamente all'inizio del conflitto in Ucraina.
Mentre, i settori maggiormente colpiti sono la pubblica amministrazione, la sanità, l'informazione e la finanza, ovvero comparti caratterizzati da elevata concentrazione di dati sensibili e infrastrutture critiche. Anche in questo caso, si nota l'elevata frequenza di attacchi informatici negli Stati Uniti rispetto a tutte le altre nazioni considerate.

Per poter constatare che l'aumento dei cyber attacchi sia effettivamente dovuto ad eventi esogeni come la pandemia e la guerra tra Russia ed Ucraina, si sono implementate due variabili dummy: la prima relativa al Covid-19 che considera l'anno 2020, mentre la seconda considera gli eventi registrati dal 2022 in poi (1= anni considerati; 0 = altrimenti).

Una volta svolta la regressione binomiale negativa con covariate le due dummy, i risultati confermano che l'aumento di attacchi cyber negli anni 2020 e dal 2022 in poi non è attribuibile a una semplice fluttuazione casuale. Infatti, la dummy relativa al Covid-19 risulta positiva e statisticamente significativa al livello 1% ($p<0,01$), indicando un incremento degli attacchi in concomitanza con l'evento. Inoltre, anche la dummy relativa alla guerra in Ucraina risulta altamente significativa ($p<0,001$), evidenziando come gli eventi geopolitici e di rilevanza globale abbiano un impatto diretto e misurabile sull'andamento dei cyber attacchi.

**Stime dei parametri**

| Parametro | P | Errore std. | 95% intervallo di confidenza di Wald | | Test sull'ipotesi | | |
|---|---|---|---|---|---|---|---|
| | | | Inferiore | Superiore | Chi-quadrato di Wald | df | Sign. |
| (Intercetta) | 2,482 | ,2339 | 2,023 | 2,940 | 112,574 | 1 | <,001 |
| [Anno=2014] | -,041 | ,1472 | -,329 | ,248 | ,077 | 1 | ,782 |
| [Anno=2015] | ,023 | ,1345 | -,241 | ,286 | ,029 | 1 | ,865 |
| [Anno=2016] | ,179 | ,1302 | -,076 | ,434 | 1,889 | 1 | ,169 |
| [Anno=2017] | ,046 | ,1341 | -,217 | ,309 | ,116 | 1 | ,733 |
| [Anno=2018] | ,003 | ,1365 | -,265 | ,270 | ,000 | 1 | ,984 |
| [Anno=2019] | ,074 | ,1297 | -,180 | ,328 | ,328 | 1 | ,567 |
| [Anno=2020] | ,345 | ,1208 | ,108 | ,582 | 8,163 | 1 | ,004 |
| [Anno=2021] | ,260 | ,1207 | ,024 | ,497 | 4,643 | 1 | ,031 |
| [Anno=2022] | ,697 | ,1146 | ,473 | ,922 | 37,020 | 1 | <,001 |
| [Anno=2023] | ,482 | ,1142 | ,259 | ,706 | 17,859 | 1 | <,001 |
| [Anno=2024] | 0[a] | . | . | . | . | . | . |

Figura 30: Effetti marginali delle variabili dummy Covid e Ucraina. Fonte: eventi registrati nel CISSM.

Dunque, appare evidente che il contesto geografico e geopolitico influenza i settori maggiormente esposti, rafforzando l'idea che la cybersecurity non è solo una questione tecnica, ma riflette dinamiche economiche, politiche e reputazionali specifiche di ciascun paese.

### 3.3.3 Esiste un effetto diretto dei cyber attacchi sul PIL di un paese?

Uno degli obiettivi di questo elaborato è di studiare come un attacco informatico possa influire sulla reputazione di un paese. Dunque, essendo la reputazione una variabile difficile da valutare e reperire, si è utilizzando il logaritmo del PIL come proxy di reputazione.

Per poter procedere nell'analisi, è stato utilizzato il data set aggregato con le variabili Paese x Anno, ed è stata creata una nuova variabile relativa al numero di attacchi con lag

(ritardo t-1 per evitare la contemporaneità). I risultati del modello misto con effetti fissi di Paese e Anno indicano che il numero di attacchi cyber non presenta un effetto significativo sul logaritmo del PIL (p = 0,170), ed anche le variabili di controllo (popolazione e utenti presenti su internet) non risultano significative. Al contrario, sia gli effetti fissi di Paese (p<0,001) sia quelli di Anno (p<0,001) sono altamente significativi, evidenziando che le differenze strutturali tra le nazioni e gli shock comuni negli anni spiegano la maggior parte della varianza del PIL. Pertanto, emerge che non vi è evidenza empirica di una relazione causale diretta tra attacchi informatici e crescita economica di un paese, ma è più corretto affermare che i paesi con elevato livello di sviluppo e integrazione digitale registrano più eventi cyber, piuttosto che questi determinino la variazione del reddito nazionale. Guardando inoltre i test F delle variabili Paese e Anno, questi rafforzano ulteriormente la teoria che le differenze strutturali tra paesi e gli shock comuni a tutte le nazioni spiegano una quota rilevante della varianza del PIL, confermando quanto emerso dalla precedente analisi.

**Test di tipo III degli effetti fissi[a]**

| Origine | GI numeratore | GI denominatore | F | Sig. |
|---|---|---|---|---|
| Intercetta | 1 | 315,000 | 4618,059 | <,001 |
| Lag_Attacchi1 | 1 | 315 | 2,052 | ,153 |
| PopolazioneMln | 1 | 315,000 | 2,283 | ,132 |
| NumeriutentisuInternetdel lapopolazione | 1 | 315,000 | ,185 | ,668 |
| Paese | 34 | 315,000 | 1223,576 | <,001 |
| Anno | 10 | 315 | 45,161 | <,001 |

a. Variabile dipendente: LogPIL.

Figura 31: Risultati modello di regressione (DV = LogPIL) con effetti fissi per paese e anno e controlli per popolazione e utenti su Internet Fonte: eventi registrati nel CISSM.

### 3.4 Discussione dei risultati

Dalle analisi empiriche emergono alcune evidenze di rilievo che confermano quanto analizzato nei capitoli teorici.

In primo luogo, i risultati suggeriscono che i paesi ad alto reddito registrano un numero significativamente maggiore di attacchi cyber rispetto alla classe di reddito medio-bassa e medio-alta. Come già affermato precedentemente, le ragioni dietro a questo fenomeno sono dovute all'elevata digitalizzazione di questi paesi, da cui consegue l'importanza e la

riservatezza delle informazioni presenti nel cyber spazio e l'esposizione a numerose vulnerabilità che attraggono attori malevoli.
Dall'altro lato, i dati mostrano anche come i paesi con reddito medio-basso riportino un numero relativamente significativo di attacchi informatici, dovuto alla maggiore vulnerabilità dei sistemi di sicurezza e piattaforme IT, e della minore capacità di investimento in misure di protezione.

In secondo luogo, l'analisi della distribuzione per settori ha evidenziato come gli attacchi informatici non si distribuiscono in modo uniforme, ma colpiscono con particolare frequenza alcuni comparti critici, quali la pubblica amministrazione, il settore sanitario, i servizi educativi, l'informazione, i servizi IT e il comparto finanziario. Questi risultati confermano quanto discusso, ovvero che gli attacchi informatici non hanno soltanto una dimensione tecnica, ma riflettono scelte strategiche degli attori coinvolti, che mirano a colpire settori economicamente e simbolicamente sensibili con effetti potenzialmente reputazionali e sistemici. In aggiunta, lo studio della tendenza temporale e l'utilizzo di variabili dummy, dimostrano come tali fenomeni non siano statici, ma si evolvono nel tempo, accentuandosi in corrispondenza di eventi globali (come la pandemia) o di specifiche congiunture geopolitiche (come i conflitti).

Infine, dall'analisi del modello misto lineare con effetti fissi per paese e anno e variabili di controllo (Popolazione e Utenti su Internet), con lag degli attacchi cyber, non emerge un impatto significativo sul PIL dell'anno precedente. Questo indica che, una volta controllate le differenze strutturali tra paesi e i fattori esogeni negli anni, non vi è evidenza empirica che gli attacchi informatici influenzino direttamente la crescita economica. Piuttosto, gli eventi cyber sembrano essere una conseguenza dell'alto sviluppo economico e digitale del paese, che determina maggiore esposizione e registrazione degli attacchi. In aggiunta, l'effetto fisso Paese e l'effetto fisso Anno sono altamente significativi, suggerendo che questi due parametri spiegano una larga parte della varianza del PIL.

Dunque, cosa suggeriscono queste conclusioni in relazione alla reputazione?

Dai risultati di queste analisi, con questi determinati dati ed informazioni, è emerso che non vi è un impatto diretto sul Prodotto Interno Lordo, ma comunque gli attacchi informatici preservano il loro peso come segnali di vulnerabilità. Infatti, la reputazione collettiva di una nazione, la fiducia nelle sue istituzioni e il suo "status" internazionale possono essere compromessi da eventi cyber, indipendentemente dagli effetti economici immediata legati al PIL. Ne consegue che, paesi con elevata digitalizzazione ed elevato reddito, essendo più vulnerabili, ed attirando più hacker, devono curare non solo la resilienza tecnica, ma anche la gestione della percezione pubblica ed internazionale.

### 3.5 Limitazioni nella ricerca e spunti per future ricerche

Sebbene si siano ottenuti risultati abbastanza in linea con i riferimenti teorici, quest'analisi non può essere considerata pienamente esaustiva e necessita di ulteriori approfondimenti.

Infatti, come già accennato nei paragrafi precedenti, sono presenti molti fattori che tendono condizionare e talvolta a limitare la portata delle ricerche ottenute.

Il primo fattore, più generico, legato all'ambito della cybersecurity mondiale, è la frammentazione dei dati e delle informazioni. Infatti, l'assenza di un dataset unico globale che raccoglie tutti gli attacchi cyber anno per anno, porta ad avere dati frammentati e incompleti.

Concentrandosi sul data set, si possono evidenziare le seguenti limitazioni:

- Il file contiene soltanto attacchi riportati pubblicamente, con un'inevitabile distorsione geografica (forte concentrazione negli Stati Uniti) dovuta sia alla maggiore trasparenza delle fonti sia alla localizzazione stessa dell'istituto che lo raccoglie.
- Come conseguenza, le osservazioni relative ad altri paesi possono non essere complete e dunque non rappresentare una visione veritiera dei fatti.
- In aggiunta, molte analisi sono state svolte con un dataset aggregato (paese x settore x anno) e questo porta ad una perdita di dettaglio a livello micro, con il rischio di non cogliere alcune dinamiche puntuali legate a singoli eventi o specifici attori.

Un ulteriore ricerca interessante che poteva essere elaborata riguarda lo studio della reputazione utilizzando la variazione del valore dei titoli in borsa come proxy di riferimento (come discusso nei capitoli teorici). Purtroppo, questa non è stata possibile a causa del numero limitato di organizzazioni quotate in borsa nel dataset CISSM. Dunque, il campione sarebbe stato troppo ridotto e poco rappresentativo per consentire una comparazione tra settori e paesi.

Inoltre, l'utilizzo di proxy alternative più accurate e dirette come gli indici di fiducia istituzionale, oppure indicatori di reputazione come il Credit Rating Sovrano o l'analisi del sentiment sui social media post attacco informatico potrebbe portare a risultati più uniformi e veritieri, ma allo stesso tempo, più difficili da reperire per un'analisi così vasta.

## CONCLUSIONI

Tramite questo elaborato si è trovata una risposta, almeno in arte, alla domanda di ricerca iniziale: “In che misura i cyber attacchi incidono sulla reputazione aziendale e sulla percezione internazionale di un paese?”

Pertanto, il lavoro di tesi ha inteso approfondire la relazione tra fattori socioeconomici, diffusione di Internet e dinamiche degli attacchi informatici nei paesi considerati, con l’obiettivo di verificarne tre ipotesi di ricerca formulate in apertura.

La prima ipotesi, relativa al legame tra la classe di reddito e la diffusione degli utenti presenti su Internet, è stata analizzata mediante un modello lineare generalizzato con distribuzione binomiale negativa. I risultati hanno mostrato come le due variabili esercitino un effetto significativo, confermando l’importanza della dimensione economica e digitale nell’esposizione al rischio cyber.
La seconda ipotesi è stata affrontata attraverso analisi descrittive, tabelle di contingenza e tesi di Monte Carlo, integrati da uno studio sul trend temporale. Le evidenze emerse segnalano differenze strutturali tra i paesi e la presenza di traiettorie evolutive specifiche, che riflettono sia fattori istituzionali sia condizioni di sviluppo tecnologico.

La terza ipotesi, verificata tramite modelli misti con inserimento del lag (t-1) del numero di attacchi, ha confermato la persistenza temporale del fenomeno: la probabilità di nuovi eventi risulta influenzata dagli attacchi precedenti, mettendo in luce la natura dinamica e non episodica del rischio cyber. Tuttavia, l’analisi del PIL come proxy di reputazione non è risultati significativa e dunque non può essere considerato un indicatore diretto della reputazione. Al contrario, sono proprio i paesi economicamente più avanzati ad attirare un numero maggiore di eventi cyber.

Nel complesso, i risultati hanno corroborato in larga parte le ipotesi di ricerca, pur con alcune differenze tra paesi e periodi, evidenziando che la dimensione economica, la diffusione digitale e la dipendenza temporale sono fattori chiave per comprendere le dinamiche degli attacchi informatici. Il contributo principale della tesi consiste nell’aver

aggiornato l'analisi con dati recenti e completi, utilizzando approcci statistici più adeguati (logaritmizzazioni, modelli misti, test di Monte Carlo), e offrendo quindi un quadro metodologico più solido.

Naturalmente, il lavoro presenta alcuni limiti: la disponibilità e la qualità dei dati restano vincolanti, così come la difficoltà di catturare variabili qualitative legate a contesti politici e istituzionali. Nonostante ciò, l'analisi fornisce spunti utili per ulteriori approfondimenti, ad esempio integrando nuove fonti di dati, ampliando l'orizzonte temporale o estendendo il confronto ad altri ambiti di rischio.

In conclusione, la ricerca ha mostrato come lo studio del rischio cyber richieda un approccio multidimensionale, capace di tenere insieme fattori economici, tecnologici e temporali. In questa prospettiva, il lavoro non solo contribuisce a una migliore comprensione del fenomeno, ma offre anche indicazioni di interesse per futuri studi e per l'elaborazione di politiche di prevenzione e gestione del rischio informatico.

**BIBLIOGRAFIA**


Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2023). *Cyber security: State of the art, challenges and future directions*. Cyber Security and Applications, 2, 100031.

Brown, R., Bailey, C., Hunt, S., Tarbitten, P., Finch, C., & Forcythe-Reid, E. (2024). *Technological advancements and hacker ingenuity: The evolution of cyber security and a zero trust model*. *Science in Parliament, 80*(2), 12–15.

Chowdhury, M. R. (2024). *Analyzing COSO Framework, Objectives, and Implementation* (Week 6 Research Paper, Purdue University Global).

Ciekanowski, M., Żurawski, S., Ciekanowski, Z., Pauliuchuk, Y., & Czech, A. (2024). *Chief Information Security Officer: A vital component of organizational information security management*. European Research Studies Journal, 27(2), 35–46.

Colleoni, E., Arvidsson, A., Hansen, L. K., & Marchesini, A. (2011). *Measuring Corporate Reputation using Sentiment Analysis*. Paper presented at the 15th International Conference on Corporate Reputation, New Orleans, United States.

Corradini, F., & Nardelli, G. (2015). *La gestione della reputazione aziendale nell'era digitale*. FrancoAngeli.

European Union Agency for Cybersecurity (ENISA). (2023, ottobre). *ENISA Threat Landscape 2023*.

European Union Agency for Cybersecurity. (2024, September). *ENISA threat landscape 2024: July 2023 to June 2024*. https://doi.org/10.2824/0710888

European Union Agency for Network and Information Security. (2017). *ENISA overview of cybersecurity and related terminology* (Version 1). https://www.enisa.europa.eu/

Fombrun, C. J., Gardberg, N. A., & Sever, J. M. (2000). The Reputation QuotientSM: A multi-stakeholder measure of corporate reputation. *The Journal of Brand Management, 7*(4), 241–255. https://doi.org/10.1057/bm.2000.10

Ftikhar, S. (2024). *Cyberterrorism as a global threat: A review on repercussions and countermeasures*. *PeerJ Computer Science, 10*, e1772. https://doi.org/10.7717/peerj-cs.1772

Ghanbari, N., & Koskinen, J. (2024). *When data breach hits a psychotherapy clinic: The Vastaamo case*. Helsinki University.

Heiding, F. (2025, 13 maggio). *72% of cyber leaders say risks are rising. Here's how states and businesses are responding*. World Economic Forum.

Hiscox Group. (2024, ottobre). *Cyber Readiness Report 2024: Protecting reputation through cyber resilience* (HSX245).

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (Year). *Cybersecurity threats and vulnerabilities: Systematic mapping study*.

International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements*.

International Telecommunication Union. (2024). *Global Cybersecurity Index (GCI): Measuring countries' commitment to cybersecurity across five pillars* [Report].

Internet Security Alliance, & Organization of American States. (n.d.). *Cyber-risk oversight handbook for corporate boards*.

Kazemi, A., Kalhornia Golkar, M., & Lajmiri, S. (2023). *Origins of cyber security: Short report*. *International Journal of Reliability, Risk and Safety: Theory and Application*, *6*(2), 77–83.

Mallick, M. A. I., & Nath, R. (2024). *Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments*. World Scientific News

OECD. (2022). *OECD Policy Framework on Digital Security: Cybersecurity for Prosperity* [Report]. OECD Publishing. https://doi.org/10.1787/a69df866-en

Ollis/Akers/Arney Insurance & Business Advisors. (2021). *Cyber case study: SolarWinds supply chain cyberattack* [PDF]. Zywave, Inc. https://ollisakersarney.com/wp-

content/uploads/2021/10/Cyber_Case_Study_-_SolarWinds_Supply_Chain_Cyberattack.pdf

Özbağ, G. K., & Çekmecelioğlu, H. G. (2019). Examining the effects of dimensions of corporate reputation on firm performance. *The European Proceedings of Social & Behavioural Sciences (EpSBS)*, *LXIV*, 271–280.

Ramezan, C. A. (2024). *The evolving role of the Chief Information Security Officer (CISO) in modern cybersecurity governance* (Doctoral dissertation, Purdue University). ProQuest Dissertations Publishing.

Siddiqui, J., & Sultana, N. (2023). Exploring enterprise risk management practices: Evidence from an emerging economy. *Journal of Accounting & Organizational Change*, 19(2), 328–353.

Wang, P., & Park, S.-A. (2017). *Communication in cybersecurity: A public communication model for business data breach incident handling*. *Issues in Information Systems, 18*(2), 136–147.

World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*. World Economic Forum

World Economic Forum. (2025, 13 gennaio). *Global Cybersecurity Outlook 2025*.

**SITOGRAFIA**


Anant, V., Donchak, L., Kaplan, J., & Soller, H. (2020, April 27). *The consumer-data opportunity and the privacy imperative*. McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

Avnet Staff. (2024, 15 marzo). *Solving the three major IoT challenges: Power supply, software fragmentation, and deployment*. Avnet. https://www.avnet.com/apac/resources/article/solving-the-three-major-iot-challenges/

Balroop, D. (2025, May 15). *Cybersecurity and IoT: Securing billions of connected devices*. LinkedIn. https://www.linkedin.com/pulse/cybersecurity-iot-securing-billions-connected-devices-dave-balroop-6aebc/

Berman, N., Maizland, L., & Chatzky, A. (2023, 8 febbraio). *Is China's Huawei a Threat to U.S. National Security?*Council on Foreign Relations. https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security

Bischoff, P. (2024, 5 giugno). *How data breaches affect stock market share prices*. Comparitech. https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/

Blue Goat Cyber. (2024, novembre 17). *Top IoT cybersecurity trends to watch in 2025*. https://bluegoatcyber.com/blog/top-iot-cybersecurity-trends-to-watch-in-2025/

BlueVoyant. (2025). *Cybercrime: History, Global Impact & Protective Measures*. https://www.bluevoyant.com/knowledge-center/cybercrime-history-global-impact-protective-measures-2022

IBM. (2024, July 30). *IBM report: Escalating data breach disruption pushes costs to new highs*. IBM Newsroom. https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs

Cimpanu, C. (2018, January 25). *Maersk reinstalled 45,000 PCs and 4,000 servers to recover from NotPetya attack*. Bleeping Computer. https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/

Cisco & Oxford Economics. (2016, maggio). *Cybersecurity as a Growth Advantage*. https://www.oxfordeconomics.com/resource/cybersecurity-as-a-growth-advantage/

Cloud Security Alliance. (2022, September 27). *The ripple effect of a data breach*. https://cloudsecurityalliance.org/blog/2022/09/27/the-ripple-effect-of-a-data-breach

Colajanni, M. (2018, 19 novembre). *Trent'anni di insicurezza digitale (1988-2018): che ci riserva il prossimo decennio?* Agenda Digitale. https://www.agendadigitale.eu/sicurezza/trentanni-di-insicurezza-digitale-1988-2018-che-ci-riserva-il-prossimo-decennio/

CSO Pakistan. (2024, 17 settembre). *ITU recognizes Pakistan's top-tier cybersecurity performance*. https://csopakistan.com/itu-recognizes-pakistans-top-tier-cybersecurity-performance/

Cyberday. (2025, 10 aprile). *Comparing EU cybersecurity frameworks: NIS2, DORA, GDPR and more*. Cyberday Blog. https://www.cyberday.ai/blog/comparing-eu-cybersecurity-frameworks

Deloitte Insights. (2023, 5 settembre). *Consumer data privacy and security*. In *Connectivity & Mobile Trends Survey 2023*. https://www.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey/2023/data-privacy-and-security.html

Directorate-General for Migration and Home Affairs. (2025, 16 giugno). *Europol published report on how cybercriminals trade and exploit data*. European Commission. https://home-affairs.ec.europa.eu/news/europol-published-report-how-cybercriminals-trade-and-exploit-data-2025-06-16_en

European Commission. (2025, 6 marzo). *Cyber Resilience Act*. In *Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

European Commission. (n.d.). *What if my company/organisation fails to comply with the data protection rules?* https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-companyorganisation-fails-comply-data-protection-rules_en

European Commission. (s.d.). *Direttiva NIS2: messa in sicurezza delle reti e dei sistemi informativi*. Plasmare il futuro digitale dell'Europa. https://digital-strategy.ec.europa.eu/it/policies/nis2-directive

European Insurance and Occupational Pensions Authority. (2024). *Digital Operational Resilience Act (DORA)*. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

Federal Bureau of Investigation. (2018, July 13). *Russian interference in 2016 U.S. elections*. FBI. https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections

Federal Bureau of Investigation. (2019, March 25). *The Melissa virus: FBI marks 20th anniversary*. FBI. https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519

gdpr.eu. (n.d.). *What are the GDPR Fines?* https://gdpr.eu/fines/

gdpr.eu. (n.d.). *What is GDPR, the EU's new data protection law?* https://gdpr.eu/what-is-gdpr/

GeeksforGeeks. (n.d.). *Difference between cyber security and information security*. https://www.geeksforgeeks.org/difference-between-cyber-security-and-information-security/

Heller, M. (2017, August 4). Ransomware recovery goes beyond data loss for enterprises. TechTarget. https://www.techtarget.com/searchsecurity/news/450423993/Ransomware-recovery-goes-beyond-data-loss-for-enterprise

https://www.youtube.com/watch?v=gwjW8Gy4Q-0

IMF. (2024, 10 ottobre). South Korea: Gross domestic product (GDP) in current prices from 1987 to 2029 (in billion U.S. dollars). Statista. https://www.statista.com/statistics/263579/gross-domestic-product-gdp-in-south-korea/

INSURICA. (2025, 25 aprile). *Cyber case study: Colonial Pipeline ransomware attack*. https://insurica.com/blog/colonial-pipeline-ransomware-attack/

Kaspar, M. (2023, 6 novembre). *The rise of cybersecurity in location decisions*. fDi Intelligence. https://www.fdiintelligence.com/content/6f72b474-145e-5eef-9079-874a0ac2a59e

Keeper Security. (2023, dicembre 27). *Common types of cybersecurity vulnerabilities*. https://www.keepersecurity.com/blog/2023/12/27/common-types-of-cybersecurity-vulnerabilities/

Laitila, A., & Mikkola, K. (2024, gennaio). *Understanding NIS2: The New EU Cybersecurity Directive*. Deloitte Finland.

Lange, K. (2023, ottobre 18). *ISACs: Information Sharing & Analysis Centers*. Splunk. https://www.splunk.com/en_us/blog/learn/isacs-information-sharing-analysis-centers.html

Leonardi, A. (2024, 25 gennaio). *Attacchi informatici: conseguenze economiche e strategie di difesa*. Cybersecurity360. https://www.cybersecurity360.it/soluzioni-aziendali/attacchi-informatici-conseguenze-economiche-strategie-difesa-business/

Lyngaas, S. (2020, 29 ottobre). *Why the extortion of Vastaamo matters far beyond Finland — and how cyber pros are responding*. CyberScoop. https://cyberscoop.com/finland-vastaamo-hack-response/

Maryville University Online. (2024, luglio 24). *The history of cybersecurity*. https://online.maryville.edu/blog/history-of-cybersecurity/

National Institute of Standards and Technology. (2018, 12 aprile). *The CSF 1.1 Five Functions*. https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions

National Institute of Standards and Technology. (2025, 3 luglio). *Cybersecurity*. In *NIST Computer Security Resource Center Glossary*. https://csrc.nist.gov/glossary/term/cyber_security

NordVPN. (n.d.). *La storia della cybersecurity*. https://www.nordvpn.com/it/blog/la-storia-della-cybersecurity/

OnSecurity Team. (2020, 13 ottobre). *Cyber Nightmare: What went wrong with Travelex and why?* OnSecurity. https://www.onsecurity.io/blog/cyber-nightmares-what-went-wrong-with-travelex/

Poma, L. (2023, 24 febbraio). *"Fake reputation": come manipolare il più prezioso degli asset intangibili di un'organizzazione*. *Creatori di Futuro*. https://creatoridifuturo.it/articoli-luca-poma/fake-reputation-come-manipolare-il-piu-prezioso-degli-assets-intangibili/

PR Newswire. (2019, ottobre 30). *Reputation accounts for 63 percent of a company's market value*. https://www.prnewswire.com/news-releases/reputation-accounts-for-63-percent-of-a-companys-market-value-300986105.html

Riskonnect. (2025, 31 gennaio). *Cost and consequences of Travelex hack could run and run*. https://riskonnect.com/cyber-security/industry-news-cost-and-consequences-of-travelex-hack-could-run-and-run/

Sjouwerman, S. (2019, September 28). *Scam of the Week: Yahoo Massive Data Breach Settlement phishing attacks*. KnowBe4. https://blog.knowbe4.com/scam-of-the-week-yahoo-massive-data-breach-settlement-phishing-attacks

Skillcast. (2025, April 22). *20 biggest GDPR fines 2018–2024: Breaches of GDPR*. Skillcast Blog. https://www.skillcast.com/blog/20-biggest-gdpr-fines

Snape, G. (2025, February 19). Supply chain cyber attacks surge over 400%, expected to continue rising – Cowbell report. *Insurance Business*. https://www.insurancebusinessmag.com/us/news/cyber/supply-chain-cyber-attacks-surge-over-400-expected-to-continue-rising--cowbell-report-525369.aspx

Sophos. (s.d.). *What is the NIS2 Directive and compliance?* https://www.sophos.com/en-us/cybersecurity-explained/what-is-the-nis2-directive-faqs

Statista. (2024, August). *Cybersecurity: market data & analysis*.

Trellix. (n.d.). *What Is Stuxnet?* https://www.trellix.com/security-awareness/ransomware/what-is-stuxnet/

U.S. Government Accountability Office. (2021, 22 aprile). *SolarWinds cyberattack demands significant federal and private-sector response (infographic)*.

Waterman, D. (2025, 16 gennaio). *Digital Operational Resilience Act (DORA)*. Diligent. https://www.diligent.com/resources/blog/digital-operational-resilience-act-dora

Werry, S., Ridgway, W. E., Simon, D. A., Kerr-Shaw, N., & Éles, K. (2024, 11 ottobre). *Navigating the new cybersecurity landscape: Key implications of the EU's NIS 2 Directive*. Skadden, Arps, Slate, Meagher & Flom

LLP. https://www.skadden.com/insights/publications/2024/10/navigating-the-new-cybersecurity-landscape

Willis, a WTW Business. (2025, maggio 27). *65 % of global corporate risk strategists identify cyber-attacks as the most significant threat to reputation, according to latest Willis survey* [Press release]. WTW. https://www.wtwco.com/en-gb/news/2025/05/65-percent-of-global-corporate-risk-strategists-identify-cyber-attacks-as-the-most-significant#:~:text=LONDON%2C%20May%2027%2C%202025

World Economic Forum. (n.d.). *Cyber risk and corporate governance*. https://www.weforum.org/projects/cyber-risk-leadership-and-corporate-governance/