Politecnico di Torino

Corso di Laurea Magistrale in Ingegneria Gestionale
Anno accademico 2024/2025
Sessione di Laurea Marzo 2025

Cybersecurity: elemento chiave per la continuità aziendale e per la crescita economica

Relatore:
Laura Abrardi

Candidato:
Gianluca Scarcia

Abstract

Nel contesto attuale in cui i singoli individui e le organizzazioni pubbliche e private si interfacciano alle numerose opportunità e minacce della sfera digitale, il ruolo della cybersecurity è sempre più cruciale. L'elaborato si pone l'obbiettivo di definire e quantificare l'impatto economico della cybersecurity sulle imprese, e di andare ad analizzare la centralità del fattore umano nelle strategie di mitigazione del rischio informatico. Sono state analizzate e proposte delle soluzioni per poter garantire una corretta sensibilizzazione, ed è stato studiato il quadro normativo dell'attuale regolamentazione in materia, per cercare di fare emergere lacune e possibili azioni da intraprendere in futuro.

Indice

Introduzione

Viviamo in un'epoca di connessioni digitali pervasive, dove la tecnologia è al centro delle attività quotidiane di individui, imprese e istituzioni. La tecnologia accompagna ogni aspetto della vita moderna, dalle interazioni personali alla gestione delle attività aziendali, fino al funzionamento delle istituzioni pubbliche. In tale contesto la cybersecurity emerge come punto strategico fondamentale, sia per proteggere i dati e le risorse, sia per garantire la continuità delle attività economiche e sociali. Il mondo delle minacce informatiche per sua natura si evolve continuamente, e diventa sempre più complesso da gestire. In tal senso le attività di sicurezza informatica sono sempre più necessarie, al fine di salvaguardare le persone, le organizzazioni, gli stati e l'immensa mole di dati generata, soprattutto nell'ultimo decennio.

Nel primo capitolo di questa tesi viene esaminato il ruolo della cybersecurity nell'attuale società, evidenziando i suoi principi fondamentali e le sue applicazioni. Viene inoltre illustrata l'evoluzione delle minacce informatiche, mettendo in risalto la complessità di un ecosistema digitale sempre più esposto a rischi. La frequenza degli attacchi mostra un trend crescente, ma soprattutto il dato più preoccupante è il fatto che si sia inasprita notevolmente la gravità media degli attacchi.

Il secondo capitolo vuole quantificare l'impatto della cybersecurity sulle imprese, evidenziando come sia diventata un elemento strategico per la competitività e la continuità aziendale. L'analisi si sofferma sui settori maggiormente colpiti dagli attacchi informatici, sui costi delle violazioni di sicurezza e sulle conseguenze gravemente dannose per la reputazione delle organizzazioni. Attraverso l'analisi del mercato attuale della cybersecurity, si dimostra come gli investimenti in cybersecurity siano fondamentali per preservare la continuità dell'attività aziendale e garantire la sostenibilità.

Il terzo capitolo si concentra sul fattore umano, il quale rappresenta contemporaneamente sia un punto di forza, sia una debolezza nella gestione della sicurezza informatica. Viene indagato il ruolo della consapevolezza e della formazione come principali strumenti di mitigazione del rischio informatico, analizzando gli innovativi programmi di educazione e sensibilizzazione digitale, i quali puntano a costruire una cultura in tale materia a tutti i dipendenti delle organizzazioni. L'obbiettivo è quello di dimostrare che il coinvolgimento attivo di tutte le persone sia il fattore chiave di successo per affrontare le insidie digitali.

Nel quarto capitolo vengono trattati il quadro normativo e le policy che regolano e supportano la cybersecurity. In particolare, viene analizzato in primo luogo l'ordinamento europeo, a seguire l'ordinamento nazionale, al fine di individuare le attuali lacune del sistema italiano. Per

completezza viene dato conto anche alle norme internazionali di certificazione in materia di sicurezza delle informazioni. Questo capitolo offre una prospettiva organica sulle misure legislative e organizzative idonee a costruire un sistema digitale resiliente e sicuro.

Questo elaborato cerca di fornire un quadro quanto più completo della cybersecurity, elemento chiave per affrontare le sfide del presente e cogliere le opportunità del futuro digitale. Tramite uno studio trasversale che tocca più discipline, quali economia e legislazione vigente, si pone l'attenzione su un tema sempre più centrale che richiama non solo l'attenzione dei governi e delle imprese, ma che richiede anche un impegno condiviso da parte di tutta la società.

1. La cybersecurity nella società moderna

Se si pensa alla realtà in cui viviamo, ci si può facilmente rendere conto che siamo immersi in ambienti costantemente "connessi e intelligenti". La maggior parte delle attività che svolgiamo sia come singoli individui sia come dipendenti di organizzazioni, dipendono sempre di più dalla sfera digitale. Con la rivoluzione digitale è possibile realizzare in rete numerose attività, come accedere alla propria banca o al servizio sanitario, molto più velocemente rispetto al passato. Come tutte le innovazioni, questi strumenti risultano ambivalenti, in quanto da un lato offrono opportunità per il progresso e l'evoluzione in campo culturale ed economico. Allo stesso tempo rappresentano un potenziale rischio perché attraverso l'utilizzo inconsapevole di questi strumenti si possono realizzare gravi violazioni dei diritti. Pertanto, vivere in una realtà interconnessa espone la comunità a una nuova serie di minacce legate al concetto di sicurezza di cui spesso non si ha nemmeno la percezione. Si considerino, per esempio le tecniche di "profilazione" e i sistemi di videosorveglianza. L'avvento del digitale implica quindi la sempre più crescente necessità di salvaguardare l'ambiente virtuale. La rete e i suoi utenti divengono sempre più frequentemente vittime di cyberattacchi, i quali non solo possono causare malfunzionamenti e interruzioni dei servizi, ma possono provocare ingenti fughe di dati.

1.1 Definizione di cybersecurity

Con il passera del tempo e con lo sviluppo di internet, la riflessione su queste domande si è concretizzato in una vera e propria disciplina, quella della cybersecurity o sicurezza informatica, intesa come tutte quelle procedure volte a proteggere la rete e i sistemi informativi, gli utenti, le organizzazioni e i loro dati dalle minacce informatiche. Gli attacchi informatici e il rischio cyber aumentano vertiginosamente ogni anno in tutti i settori, poiché ormai i dati personali e aziendali sono costantemente esposti a minacce, essendo diventati uno dei beni più preziosi per le organizzazioni.

"La cybersecurity è la seconda emergenza in Europa, dopo il cambiamento climatico e prima dell'immigrazione"

Lo ha detto il presidente della Commissione Europea Jean-Claude Junker il 13 Settembre 2017 [2]. La cybersecurity infatti è uno dei principali rami in cui le aziende investono in tecnologia e formazione dei dipendenti ed è uno dei principali temi su cui si stanno concentrando le istituzioni. La cybersecurity è indispensabile per proteggere le informazioni personali private, ma anche dati aziendali, governativi e infrastrutture critiche. Viene definita come la disciplina dedicata alla difesa dalle relative minacce di tutte le infrastrutture digitali, e di tutte le informazioni che proliferano

nella rete. Una conseguenza è il fatto che tale disciplina sia finalizzata a proteggere i dati degli utenti delle reti e dei sistemi informativi. Per prevenire e rispondere a tali minacce si possono intraprendere diverse strategie, ad esempio mediante la crittografia dei dati e i software antivirus.

La cybersecurity è un campo di applicazione di un concetto più ampio e generale: il Cyberspace. "Il Cyberspace è un dominio globale e dinamico caratterizzato dall'uso combinato di uno spettro elettronico ed elettromagnetico, con lo scopo di creare, immagazzinare, modificare, scambiare, condividere, estrarre, utilizzare, eliminare informazioni, gestire e compromettere beni fisici". Questo sistema di reti digitali è un nuovo fronte culturale ed economico, un mondo in cui multinazionali, organizzazioni e criminali informatici si sfidano per conquistare dati e informazioni. L'ambiente virtuale permette di accedere a tutte le informazioni raccolte nei database, permettendone lo scambio tra più utenti. Come aveva pensato Gibson[1], il cyberspazio oggi è definito come un ambiente costituito da un insieme di software, hardware, utenti, big data[2] e tutte le relazioni che esistono tra loro. Tuttora questi processi si realizzano e si evolvono continuamente attraverso internet che, da mezzo di interazione e condivisione, è diventato il mezzo di gran parte delle operazioni politiche, sociali, economiche e commerciali.

La cybersecurity, come si è potuto capire dai passi precedenti, è una disciplina legata agli ultimi trent'anni. Infatti, si fa attribuire la sua nascita attorno agli anni '70, quando iniziarono a diffondersi i primi programmi informatici. Di seguito sono elencati i marco-eventi storici di tale materia:

- La sicurezza informatica ebbe inizio negli anni Settanta, quando il ricercatore Bob Thomas creò un programma informatico chiamato Creeper in grado di muoversi attraverso la rete ARPANET, lasciando una scia di tracce ovunque andasse. Ray Tomlinson[3] scrisse il programma Reaper, che inseguiva e cancellava Creeper. Reaper fu il primo esempio di software antivirus e il primo programma autoreplicante, il che lo rese il primo virus informatico in assoluto.

- Il 1987 è stato l'anno di nascita degli antivirus commerciali.

- Con la diffusione di internet, un aumento sempre maggiore di persone inizia a mettere online le proprie informazioni personali. Le entità del crimine organizzato videro in questo fenomeno una potenziale fonte di guadagno e iniziarono a rubare dati da persone e governi

[1] William Gibson (Conway, 17 marzo 1948) è uno scrittore e autore di fantascienza statunitense naturalizzato canadese.
[2] In statistica e informatica, la locuzione inglese big data ("grandi dati") o talvolta l'italiana mega-dati indicano genericamente una raccolta di dati informatici così estesa in termini di volume, velocità e varietà da richiedere tecnologie e metodi analitici specifici per l'estrazione e l'analisi.
[3] L'inventore della posta elettronica

attraverso il web. A metà degli anni 90, le minacce alla sicurezza della rete sono aumentate in modo esponenziale e per proteggere il pubblico è stato necessario produrre in massa firewall e programmi antivirus

- All'inizio degli anni 2000 le organizzazioni criminali hanno iniziato a finanziare pesantemente i cyberattacchi professionali e i governi hanno iniziato a dare un giro di vite alla criminalità informatica, infliggendo pene molto più grandi ai colpevoli. La sicurezza informatica ha continuato a progredire con la crescita di Internet, ma anche dei virus.

- Oggi il settore della sicurezza informatica continua a crescere alla velocità della luce. La cybersecurity è un tema divenuto ormai di rilevanza strategica per tutti i paesi: dalle dinamiche legate alla difesa e alla sicurezza , alla politica industriale e all'avanzamento tecnologico, fino alle implicazioni geopolitiche.

La cybersecurity è un ambito multi sfaccettato che continua ad evolvere e diversificarsi nel corso del tempo. Infatti, ciascuna di queste specializzazioni è indispensabile per la protezione di un ecosistema digitale. Di seguito vengono discussi i principali campi di applicazione:

- La sicurezza della rete: essa ha l'obbiettivo di proteggere i dati lungo tutte le fasi del loro ciclo di vita, cercando di non permettere agli utenti non autorizzati di accedere a determinate informazioni. Per permettere ciò sono necessarie diverse procedure da attuare, tra le quali le più significative sono il corretto utilizzo di software antivirus, controllo del traffico di dati in rete e il controllo di accesso, ad esempio tramite robuste procedure di autenticazione e sistemi di password forti.
- La sicurezza delle applicazioni: essa è la disciplina volta a proteggere le applicazioni mobili, le quali risultano un'importante canale di accesso per utenti e malintenzionati. La sua funzione è quella di difendere le applicazioni lungo tutta la loro vita, fin dalle fasi di progettazione, e di studiare possibili falle e vulnerabilità che i malintenzionati potrebbero sfruttare. Alla base di questa disciplina c'è la crittografia dei dati e il monitoraggio dei sistemi tramite test.
- La sicurezza delle operazioni: è la disciplina volta a proteggere l'infrastruttura IT dei processi operativi aziendali, ad esempio legati ai sistemi informativi legati alla produzione, ai sistemi gestionali, ai sistemi di magazzino, ai sistemi di contabilità e molti altri. Le attività dei malintenzionati informatici possono avere conseguenze molto gravi su attività aziendali, ad esempio possono causare blocchi della produzione, fuga di dati aziendali e dei clienti, o addirittura blocco totale dei sistemi informatici in

cambio di ingenti riscatti. Questo aspetto verrà approfondito nel prossimo capitolo, poiché ormai tutte le tipologie di organizzazioni devono adottare importanti strategie di mitigazione del rischio informatico. Non adottare delle corrette strategie di prevenzione può causare gravissimi danni patrimoniali, costi e impattare sulla reputazione di tutti gli *stakeholders*.

- La sicurezza Cloud: il cloud computing è una tecnica sempre più diffusa per l'archiviazione dei dati, poiché permette l'accesso in temo reale ad una grandissima mole di dati e riduce i costi di infrastrutture IT, poiché altrimenti dovrebbero essere gestite internamente dalle organizzazioni. Questo però aumenta i rischi legati all'acquisizione di questi dati, ad esempio da utenti di terze parti. Questa disciplina è finalizzata a proteggere la proliferazioni di queste attività di dati e a tutelare gli utenti autorizzati. Per rendere possibile ciò si possono adottare complesse strategie di backup di dati e sistemi, controlli di accesso e delle attività, e piani di risposta in caso di problemi o minacce.
- La sicurezza dell'utente finale: l'utente finale rappresenta il punto più vulnerabile della sicurezza informatica. Questo perché, come approfondiremo successivamente nel capitolo tre, non sempre è adeguatamente consapevole dei rischi associati alla sua attività online, sia per la sua incolumità sia per quella della sua organizzazione. L'adozione di pratiche che lo tutelino e lo rendano consapevole dei rischi informatici, ad esempio tramite l'utilizzo di best practice, password forti, backup dei dati, reti sicure VPN e molto altro, sono alla base di tale disciplina. Anche in questo caso il controllo dell'attività sospetta e degli accessi risulta fondamentale.

Ogni strategia di gestione della cybersecurity si basa sui tre principi fondamentali già citati precedentemente: confidenzialità, integrità e disponibilità dei dati:

a) Confidenzialità (o Privacy): essa consente ai dati e le risorse di essere preservate dal possibile utilizzo o accesso da parte di utenti estranei non autorizzati e tipicamente malintenzionati. Questa deve essere garantita lungo tutta la vita del dato, dalla sua archiviazione, durante l'utilizzo e in transito nella rete.
b) Integrità: è relativa alla capacità di garantire la correttezza dei dati e delle risorse e assicurare che non siano modificate o cancellate per nessuna ragione, se non da soggetti autorizzati.
c) Disponibilità: tale concetto è finalizzato a permettere agli utenti autorizzati di accedere alle funzionalità di cui hanno bisogno per un intervallo di tempo desiderato. Ne consegue che

bisogna evitare interruzioni di servizio e garantire che le infrastrutture siano pronte per la corretta offerta di servizi.

Per comprendere bene cosa si intenda con la nozione di Cybersecurity, bisogna distinguere tra Cyber Security e Information Security [Figura 1]. Questi due termini spesso sono considerati sinonimi, tuttavia differiscono per diversi aspetti.

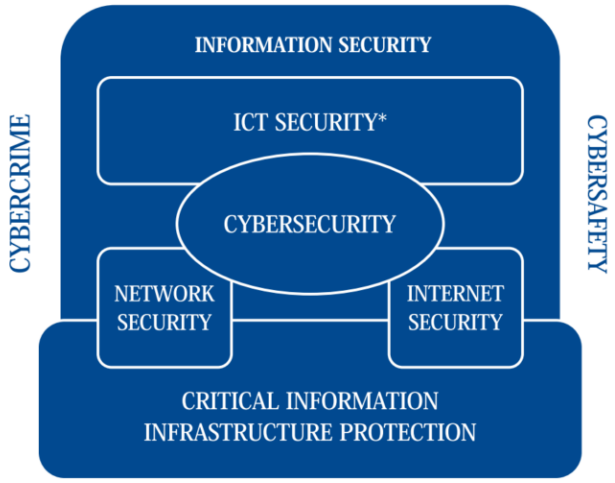

Figura 1: Diagramma concettuale cybersecurity

L'Information Security e la Cyber Security sono materie strettamente connesse che si occupano di proteggere le informazioni, ma si differenziano nella loro applicazione. La Sicurezza dell'Informazione si occupa di proteggere tutte le forme di informazione, indipendentemente dalla loro natura fisica o digitale. La Cyber Sicurezza si concentra sulla protezione delle informazioni digitali e dei sistemi informativi.

L'information Security si occupa di proteggere la disponibilità, l'integrità e la confidenzialità delle informazioni di qualsiasi organizzazione. Risulta fondamentale nel mondo digitale in cui viviamo e operiamo, perché le informazioni sono sempre preziose e proprio per questo sempre più vittime di attacchi informatici. L'Information Security propone una serie di misure che devono essere messe in atto per prevenire, rilevare e rispondere alle minacce a cui i dati sono sottoposti. Questo significa ad esempio implementare in azienda il controllo degli accessi, una gestione sicura delle password e l'uso consapevole dei dispositivi. Inoltre contribuisce alla formazione continua dei dipendenti, al fine di promuovere sempre di più le pratiche per la sicurezza delle informazioni. È fondamentale quindi avere una strategia più chiara possibile e continuamente aggiornata che comprenda la protezione individuale e collettiva, la gestione dei rischi e la conformità normativa [3].

La Cybersecurity si concentra sulla protezione di tutta la sfera IT presente in azienda e in generale delle reti, per prevenire possibili attacchi e intrusioni informatiche. L'obiettivo è quello di mantenere al sicuro le risorse digitali, contrastando gli accessi non autorizzati che potrebbero acquisire dati e divulgarli per scopi criminosi o di lucro. Anche la attua una serie di strategie architettate per diminuire i rischi associati alle attività online:

- Identificazione e autenticazione per dare accesso ai *tools* solo alle persone autorizzate.
- Protezione da malware, installando software antivirus e anti malware, al fine di contrastare il più possibile le moderne tecniche di attacco informatico.
- Monitoraggio delle attività sospette attraverso software specifici in grado di controllare le reti e le attività degli utenti, così da rilevare in anticipo le minacce e rispondere in maniera corretta e tempestiva.
- Protezione delle reti. È importante che ci sia una configurazione corretta di firewall e dispositivi che dovranno proteggere la rete da accessi non autorizzati.
- Una corretta gestione delle vulnerabilità dei sistemi, in modo tale da coprire eventuali falle utilizzabili da malintenzionati.

L'Information Security si riferisce quindi alla protezione delle informazioni in qualsiasi forma. Possono essere digitali, ma anche fisiche, andando così a interessare una protezione dei dati completa. La Cyber Security, al contrario, come dice l'etimologia, si concentra sulla protezione delle informazioni digitali, dei sistemi informatici e delle reti da minacce informatiche. La Cyber Security è un sottoinsieme dell'Information Security, andandosi a concentrare sulle minacce cyber e la protezione dei dati digitali, mentre la Sicurezza dell'Informazione si concentra su una più vasta gamma di dati, inclusi documenti fisici, informazioni sensibili e informazioni riservate [4]. Per concludere, quindi, la Cyber Security e l'Information Security garantiscono la sicurezza di tutte le informazioni e i dati aziendali e non solo, adottando strategie complete che tengano conto sia dei dati fisici sia di quelli digitali.

1.2 La crescita esplosiva delle minacce informatiche

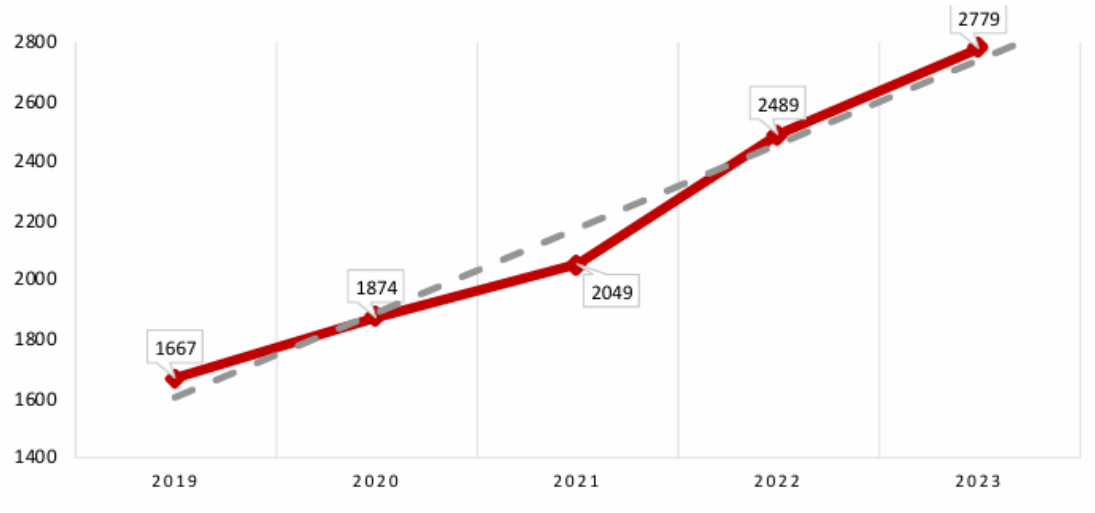

Figura 2: Frequenza degli attacchi informatici noti a livello globale [5]

L'ascesa delle minacce informatiche è un motivo primario per l'aumento dell'attenzione alla cybersecurity. Come si può vedere [Figura 2] ogni anno il numero di attacchi informatici tende ad aumentare: si può notare che nell'ultimo anno ci sono stati quasi 3000 attacchi, il numero maggiore di sempre, e come mostra il grafico già dal 2019 i casi reali hanno superato le previsioni in grigio, ossia la linea di tendenza. Si può quindi notare un forte trend crescente negli ultimi quattro anni. A conferma di una costante crescita dello scenario degli incidenti, la frequenza è aumentata di più del 50% rispetto a dieci anni fa.

Le minacce alla sicurezza informatica sono molteplici e spesso derivano dalla diffusione delle nuove tecnologie. Il Cyber-Crime comprende tutte quelle attività criminose che sul web e altre tecnologie digitali per delinquere, come pretendere un riscatto o rubare informazioni riservate, di queste attività gli attacchi hacker sono solo alcuni esempi. Tuttavia, spesso si tende a confondere minaccia, vulnerabilità e rischio. Il primo termine indica un potenziale evento finalizzato ad intaccare la sicurezza, il secondo identifica un punto debole che può essere sfruttato per generare un attacco, invece il terzo è l'effettiva concretizzazione di un attacco e le rispettive conseguenze che ne derivano, come i danni patrimoniali e d'immagine.

Secondo l'Agenzia Europea per la Cybersicurezza un *cyber attack* comprende *"tutti gli incidenti informatici scatenati da un intento malevolo, in cui si verificano danni, interruzioni o disfunzioni"*[4]. In altri termini, questi incidenti di sicurezza si sostanziano nella presa di mira da parte di malintenzionati di uno o più elementi della sicurezza informatica. L'esempio più impattante è

[4] Definizione di attacco cyber secondo l'Agenzia Europea per la sicurezza informatica

costituito dai data-breach [5] definiti dal Garante per la protezione dei Dati personali (GPDP) come una violazione della sicurezza che implica la compromissione di dati personali trasferiti o elaborati in qualsiasi modo tramite la loro distruzione o modifica non autorizzate, o il loro smarrimento o divulgazione non consentita mediante l'accesso illecito. Questo perché i dati ormai rappresentano un vero e proprio asset fondamentale per le imprese. Un eventuale violazione comporta danni ingenti per l'azienda vittima, sia in termini economici sia di immagine. Questo aspetto verrà approfondito nel capitolo due dell'elaborato.

Il Rapporto Clusit[6] definisce quattro tipologie di attaccanti[7] [5]:

- Il **cybercrime** (crimine informatico) si riferisce a qualsiasi attività illegale che viene svolta utilizzando o prendendo di mira dispositivi digitali, reti o sistemi informatici. Gli obiettivi principali sono solitamente il guadagno finanziario o il furto di dati. Esempi: Ransomware e frodi online.
- L'**hacktivism** consiste nell'utilizzo di tecniche informatiche per diffondere informazioni di natura sociale o politiche. Questi fenomeni mirano destabilizzare il pubblico o a protestare con le istituzioni, come ad esempio gli attacchi DDoS[8].
- L'**espionage** (spionaggio informatico) è l'uso di metodi di informatici criminali per trovare informazioni segrete da individui, aziende o governi. Le cause alla base possono essere molteplici, come analisi di concorrenza e analisi governative. Esempi: Spionaggio industriale per vantaggi strategici e competitivi.
- **L'Information Warfare** è l'uso criminoso della diffusione di informazioni e della tecnologia per influenzare, manipolare o ostacolare un avversario o competitor, spesso a livello governativo o militare. Esempi: Propaganda digitale, sabotaggio informatico contro infrastrutture critiche, operazioni di disinformazione durante conflitti geopolitici.

Le motivazioni dietro a questi attacchi sono vastissime, e ancora oggi alcune risultano ignote. Il grafico seguente [Figura 3] rappresenta la distribuzione di queste tipologie: la distribuzione degli attaccanti tra il 2019 e il 2023 mostra che il cybercrime è la principale causa di attacchi, con una crescita del 13% rispetto all'anno precedente. Tale trend è confermato dagli analisti, secondo cui esiste una commistione crescente tra criminalità tradizionale e cybercrime, che porta a reinvestire

[5] In italiano violazione dei dati
6 Associazione italiana per la sicurezza informatica
[7] In materia di sicurezza informatica, l'attaccante viene definito un'entità che si insinua in ambienti informatici al fine di rubare denaro, informazioni e in generale attività criminali.
[8] Distributed Denial of services

i profitti in attività digitali. Al contrario, gli attacchi legati allo spionaggio e alla guerra informativa hanno un trend decrescente: gli episodi di spionaggio sono calati da 259 nel 2022 a 178 nel 2023, mentre quelli di information warfare sono scesi da 103 a 46. Parallelamente si registra un forte incremento degli attacchi di hacktivism, che sono quasi triplicati, passando da 84 nel 2022 a 239 nel 2023, indicando una crescita delle attività a sfondo politico e sociale.

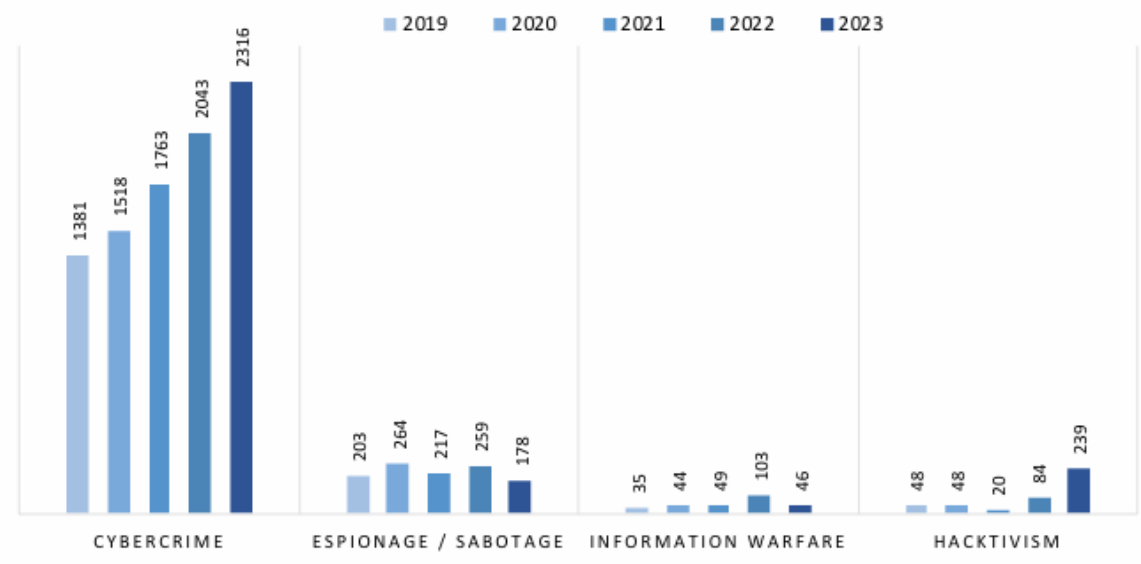

Figura 3: Distribuzione degli attaccanti [5]

È importante tuttavia cercare di valutare la severità di ogni tipologia di attaccante: il grafico seguente [Figura 4] evidenzia un'evoluzione significativa nella severità degli incidenti causati dal cybercrime, mostrando che, indipendentemente dal numero totale di attacchi, gli incidenti nel 2023 hanno avuto conseguenze più critiche. In particolare, gli attacchi con impatti critici nel 2023 sono aumentati in tutte le categorie principali. Nel caso dello spionaggio e dell'information warfare, gli attacchi con impatti critici sono aumentati notevolmente, passando da circa il 50% nel 2022 a circa il 70% nel 2023. Questo trend può essere spiegato in gran parte dai conflitti geopolitici come la guerra Russo-Ucraina e il conflitto Israelo-Palestinese, nei quali molti Paesi sono coinvolti anche sul piano della cyber security, con impatti critici maggiori. Per quanto riguarda l'hacktivism, invece, si osserva solamente un 10% di attacchi critici. Questo è dovuto al forte aumento degli attacchi in questa categoria, che, pur avendo un impatto medio o alto, tendono ad avere obiettivi più dimostrativi, con effetti meno devastanti rispetto ad altri tipi di attacchi cyber. Questo scenario riflette un contesto geopolitico sempre più teso, ma anche la natura meno distruttiva degli attacchi, che non sono mirati a danneggiare gravemente ma a inviare un messaggio geo-politico. In generale, per tutte le categorie osservate, gli attacchi a basso impatto sono praticamente scomparsi, riflettendo una tendenza crescente verso attacchi sempre più gravi e mirati.

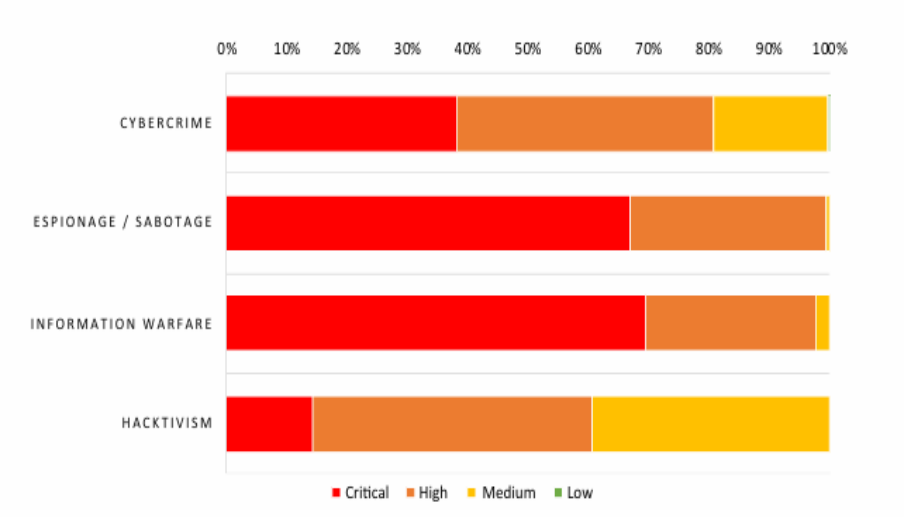

Figura 4: Severity per attaccanti 2023[5]

Le recenti statistiche sulla cybersecurity mostrano che le organizzazioni e le persone sono vittime di diverse tipologie di attacchi informatici, tra cui i più diffusi sono i seguenti:

1. **Malware**: si tratta di programmi progettati da criminali per infettare dispositivi, sistemi informativi, rubare credenziali di accesso, codici di carte di credito e molto altro ancora. I virus sono la loro forma più diffusa, e corrispondono a file progettati per influire sulle prestazioni dei devices, corrompere i file e impedire agli utenti di accedere ai dispositivi.
2. **Cavalli di Troia o trojan**: sono software dannosi che consentono ad altri malware di accedere ad un determinato hardware. Si mascherano da software legittimi per ingannare l'utente e ottenere accesso al sistema informatico, per iniziare una qualsiasi attività criminosa.
3. **Spyware**: sono programmi che si insediano nei dispositivi con diverse tecniche di hacking per controllare l'attività degli utenti e tutti i loro dati. Ciò consente agli aggressori di reperire dati sensibili, come informazioni su carte di credito, credenziali di accesso e password per essere utilizzate come ricatto.
4. **Ransomware**: un ransomware è un tipo di malware progettato per bloccare o limitare l'accesso a un sistema informatico o ai file in esso contenuti, in modo da costringere la vittima a pagare un riscatto per riottenere l'accesso. Il ransomware infetta un dispositivo, crittografa i dati o blocca il sistema e poi mostra un messaggio in cui chiede un pagamento per fornire la chiave di decrittazione o per sbloccare il sistema.

   Ci sono diverse tipologie di ransomware, ma generalmente funzionano in due modi:

   - Ransomware di crittografia: riescono a bloccare ingenti quantità di file rendendoli accessibili solo tramite apposite operazioni di decrittazione. La vittima riceve poi

una richiesta di riscatto per ottenere la chiave di decrittazione necessaria a ripristinare i file.
    - Ransomware di blocco: blocca il dispositivo in modo che l'utente non possa accedere al sistema, senza necessariamente criptare i file. In genere, viene mostrata una schermata con le istruzioni per il pagamento.
5. **Adware**: sono annunci indesiderati che compaiono tipicamente durante l'utilizzo di un browser web. L'adware è spesso collegato ad applicativi dannosi, che possono essere installati sui devices degli utenti che hanno accidentalmente lanciato tale applicativo.
6. **Botnet**: spesso utilizzati per commettere attacchi di massa, riescono a corrompere una grande serie di dispositivi. Essi riescono ad agire perché attaccano direttamente i server centrali, e quindi riescono ad infettare molti utenti di tale rete.
7. **Phishing o Social engineering**: tramite e-mail, messaggi di testo e messaggi social, gli aggressori ingannano le vittime, spesso inducendole a entrare in link oppure scaricare allegati che si rifanno a siti web falsi e conseguentemente dannosi. Ciò consente loro di rubare dati di utenti, password, dati di carte di credito ecc
8. **Attacchi Man in the Middle**: si tratta di una tipologia di attacco in virtù del quale aggressori riescono a sfruttare dei punti deboli dei sistemi al fine di estorcere e rubare dati. Il nome deriva proprio dal fatto che consente agli aggressori di insinuarsi tra gli utenti delle reti e dei sistemi.

Nel 2023, il malware-ransomware è stata la tecnica di attacco più utilizzata dai cybercriminali, rappresentando il 36% dei casi [Figura 5]. Questo tipo di malware è scelto per la sua elevata redditività economica per gli aggressori. Al secondo posto troviamo lo sfruttamento delle vulnerabilità o falle dei sistemi (18%), che includono sia vulnerabilità note che quelle più insidiose, come gli attacchi tramite "zero-day", che sfruttano falle non ancora scoperte o divulgate. Un altro 20% degli attacchi riguarda tecniche sconosciute, per le quali non sono ancora note le tecniche utilizzate.

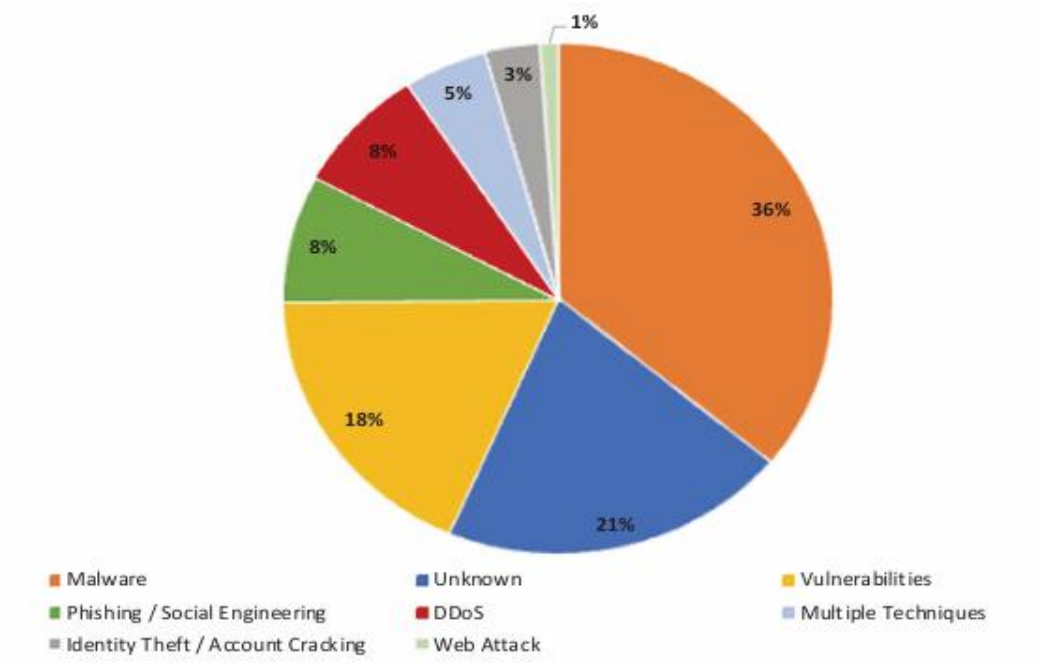

Figura 5: Istogramma percentuale delle tipologie di cyber-attacks nel 2023 [5]

Il seguente grafico conferma un trend in crescita per quasi tutte le tipologie di attacco [Figura 6]. In particolare mostra una crescita degli attacchi malware, in termini numerici arrivati a 1002, rispetto ai 910 del 2022. Per quanto riguarda lo sfruttamento delle debolezze dei sistemi informatici, si stimano 510 attacchi. Invece gli attacchi DDoS ammontano a 220, raggiungendo quasi il doppio del 2022.

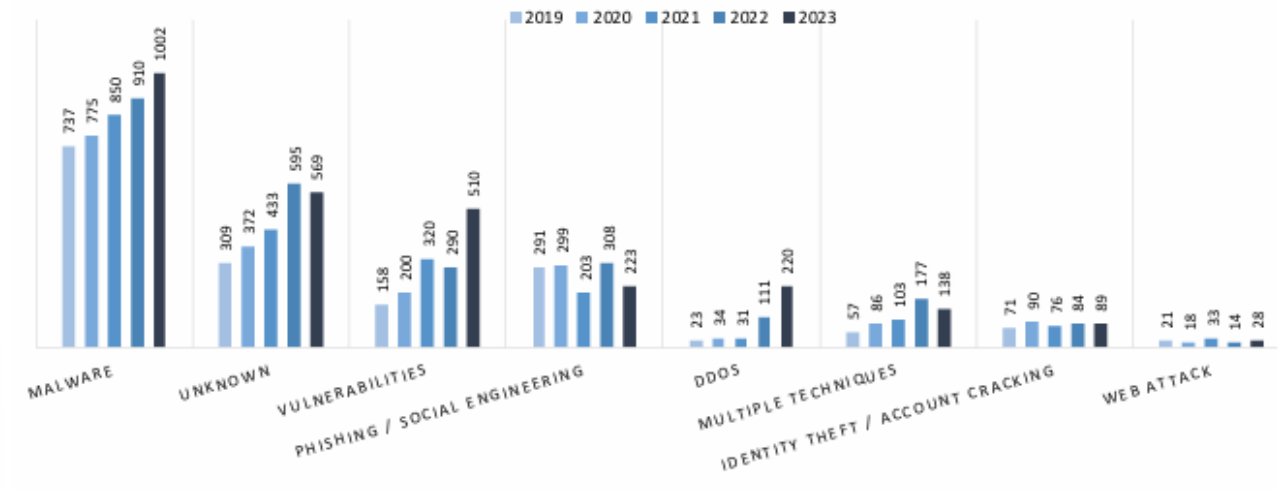

Figura 6: Andamento degli attacchi informatici 2019-2023[5]

Tuttavia, se si considerano le percentuali sul totale si riescono a fare valutazioni più complete. Infatti, dal grafico sottostante [Figura 7] si possono osservare alcuni trend importanti nell'evoluzione delle tecniche di attacco. Nonostante il numero assoluto di attacchi basati su

malware continui a crescere, la sua incidenza percentuale sul totale degli attacchi sta diminuendo, consolidando un trend che si è già manifestato negli anni passati. Al contrario, gli attacchi DDoS mostrano una crescita continua (+4 punti percentuali rispetto all'anno precedente), così come gli incidenti legati allo sfruttamento delle vulnerabilità (+6 punti percentuali). Il phishing e il social engineering, pur vedendo una diminuzione (-4 punti percentuali), restano tecniche rilevanti, suggerendo che, nonostante la riduzione, siano ancora aree problematiche che necessitano di attenzione, specialmente in termini di sensibilizzazione degli utenti. Inoltre, il ricorso a tecniche multiple diminuisce anch'esso (-2 punti percentuali), mentre l'uso di tecniche come il furto di identità e il cracking di account resta stabile al 3% del totale degli attacchi, così come gli attacchi web (1%). Infine, c'è una riduzione nell'incidenza degli attacchi basati su tecniche sconosciute, sebbene il monitoraggio di questi attacchi resti necessario. Un aspetto emergente da tenere sotto osservazione è l'utilizzo crescente dell'intelligenza artificiale (AI) da parte dei cybercriminali. L'AI viene impiegata per selezionare target, scansionarli alla ricerca di vulnerabilità note, analizzare il codice per individuare nuove falle, e produrre contenuti per phishing o codici per malware. Questo è un trend in rapida ascesa, i cui effetti si vedranno con maggiore chiarezza nel futuro prossimo.

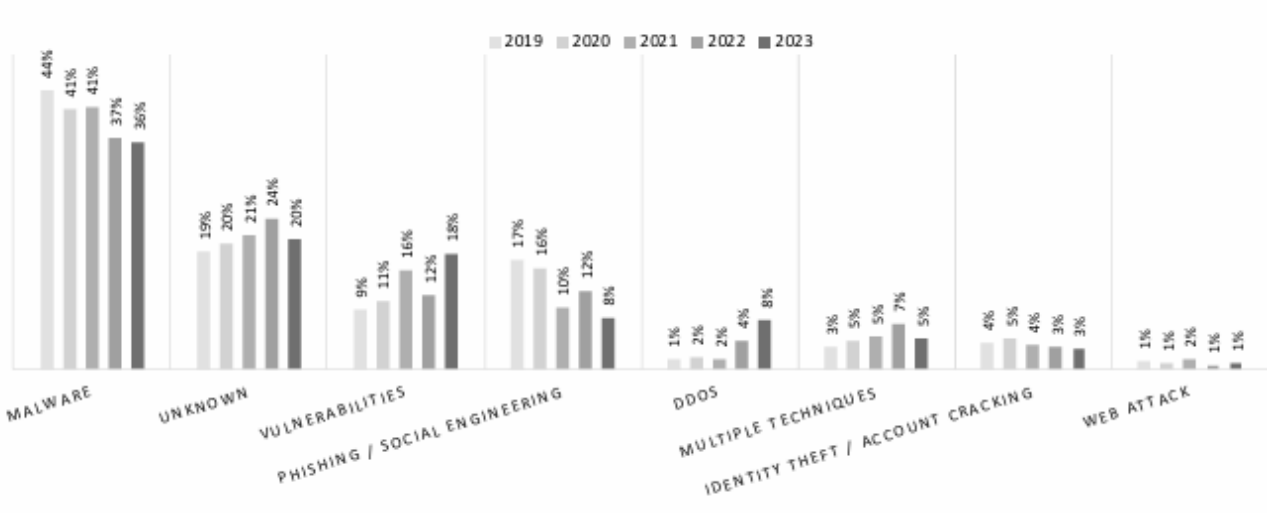

Figura 7: Tecniche di attacco in % 2019-2013 [5]

Procedendo con una valutazione della gravità degli attacchi, si può notare un incredibile aumento di severità in ogni tipologia di attacco. Diversamente rispetto al 2022 [Figura 8], il 2023 ha visto un aumento della percentuale di criticità degli attacchi [Figura 9]. Il malware mostra un andamento costante, pari al 40% di criticità, mentre lo sfruttamento delle vulnerabilità ha visto un significativo aumento di criticità, arrivando al 50%. Anche la percentuale di criticità del phishing e del cracking risulta costante. Un dato preoccupante invece risulta il fatto che sia incrementata la severity critica dovuta a tecniche sconosciute, arrivando al 40%.

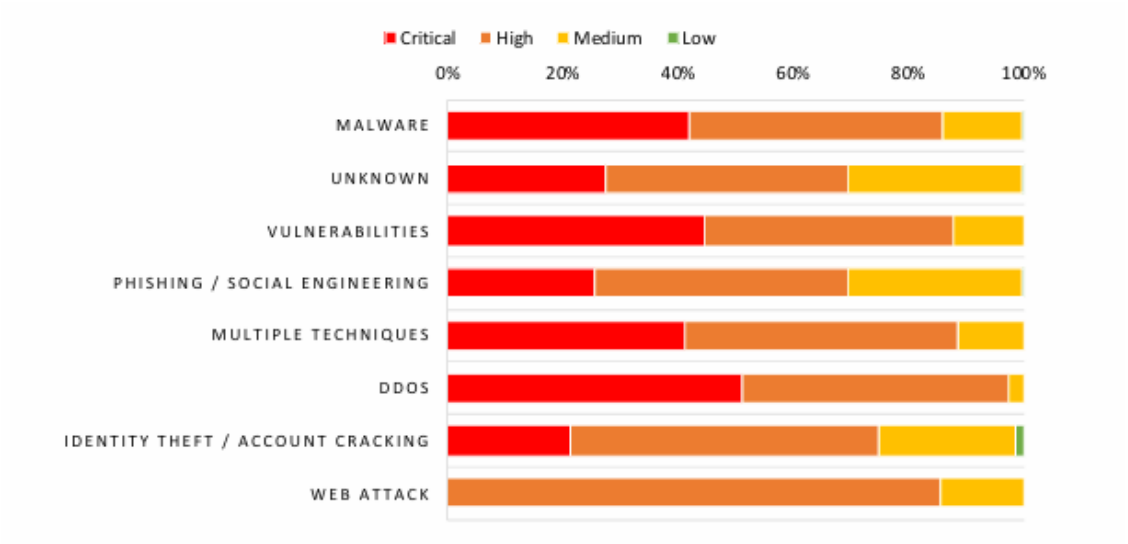

Figura 8: Severity per tipologia di attacco 2022 [5]

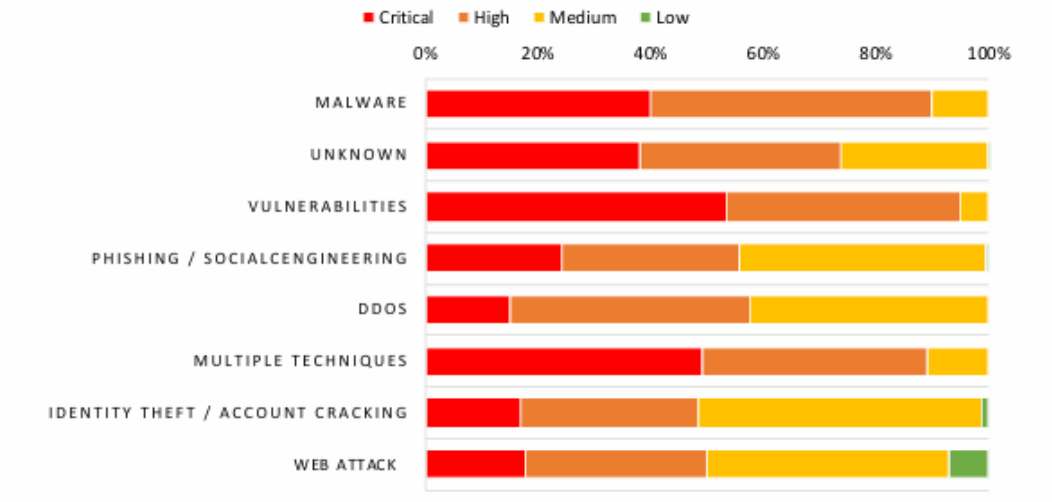

Figura 9: Severity per tipologie di attacco 2023[5]

2. L’impatto della cybersecurity sulle imprese

Come si è potuto evincere dal capitolo precedente, una costante del mondo attuale, sia per le organizzazioni, sia per le persone fisiche, è sicuramente il ruolo centrale del dato. Molti studi affermano che nove dati su dieci siano stati generati negli ultimi due anni. Questo trend esponenziale obbliga le organizzazioni a stravolgere e modernizzare la gestione e l’utilizzo dei dati, al fine di migliorare la loro attività. I dati sono diventati un asset fondamentale delle imprese, a testimonianza di ciò si pensa che i dati saranno la misura chiave per capire se un'impresa resterà rilevante attraverso la rivoluzione digitale [6]. Una conseguenza di quest’ipotesi sarà il fatto che le imprese più performanti saranno quelle che avranno adottato le migliori pratiche di gestione dei dati. Le grandi multinazionali stanno già iniziando tale rivoluzione, infatti molte hanno iniziato a inserire figure di sicurezza informatica all’interno dei consigli di amministrazione. Le potenzialità di una corretta gestione dei dati sono innumerevoli, ad esempio è possibile monitorare in tempo reale le prestazioni aziendali, aumentare il valore aggiunto in ogni singola attività e contribuire alla catena del valore.

Grazie alla corretta gestione dei dati, quindi, si può ottenere una vastissima serie di vantaggi:

- insight più approfonditi e previsioni più accurate
- migliore comprensione di ciò che i clienti desiderano
- offerta di *customer experience* ottimizzata
- nuovi modelli di business.

Questo immenso patrimonio di dati, purtroppo, è diventato un bersaglio per le organizzazioni criminali e non solo, infatti ormai sono sempre più frequenti tipologie di attacchi informatici sempre più evolute e difficili da intercettare e fermare. Questa era la premessa per comprendere l’importanza della cybersecurity per le imprese di qualsiasi settore.

2.1 Analisi dei settori più colpiti

Oggigiorno tutti i settori industriali sono vittima di attacchi informatici e risulta impossibile essere completamente immuni da tali minacce, tuttavia, analizzando i dati, si è potuto osservare che esistono settori più colpiti di altri. Il grafico seguente [Figura 10] rappresenta i dieci settori più colpiti da cyber attacks tra il 2019 e il 2023. L'analisi della distribuzione delle vittime degli attacchi evidenzia una riduzione dell'incidenza complessiva degli attacchi verso bersagli multipli, con una diminuzione di 3 punti percentuali rispetto al 2022. Per “bersagli multipli” ci si riferisce ad attacchi che colpiscono più obbiettivi o settori contemporaneamente, con tecniche simili, senza concentrarsi

su un settore specifico. Di contro, si registra un aumento degli attacchi al settore sanitario (+2 punti percentuali) e finanziario/assicurativo (+3 punti percentuali) [5].

Anche i settori delle scuole, manifattura, trasporti/logistica e commercio all'ingrosso e al dettaglio aumentano la percentuale rispetto al 2022. L'industria manifatturiera ha visto una crescita costante dal 2019, raggiungendo il picco con un'incidenza passata dal 2% al 6% degli attacchi totali in un quinquennio. Nel 2023 invece sono rimaste costanti i settori governativi, militari e scientifici. Gli attacchi al settore ICT, invece, hanno mostrato una diminuzione costante dal 2020 pur essendo una quota di poco maggiore del dieci percento delle vittime totali. Complessivamente i settori dei trasporti e commercio all'ingrosso e al dettaglio rappresentano insieme il 9,1% degli attacchi; tra questi i settori trasporti e commercio sono in crescita.

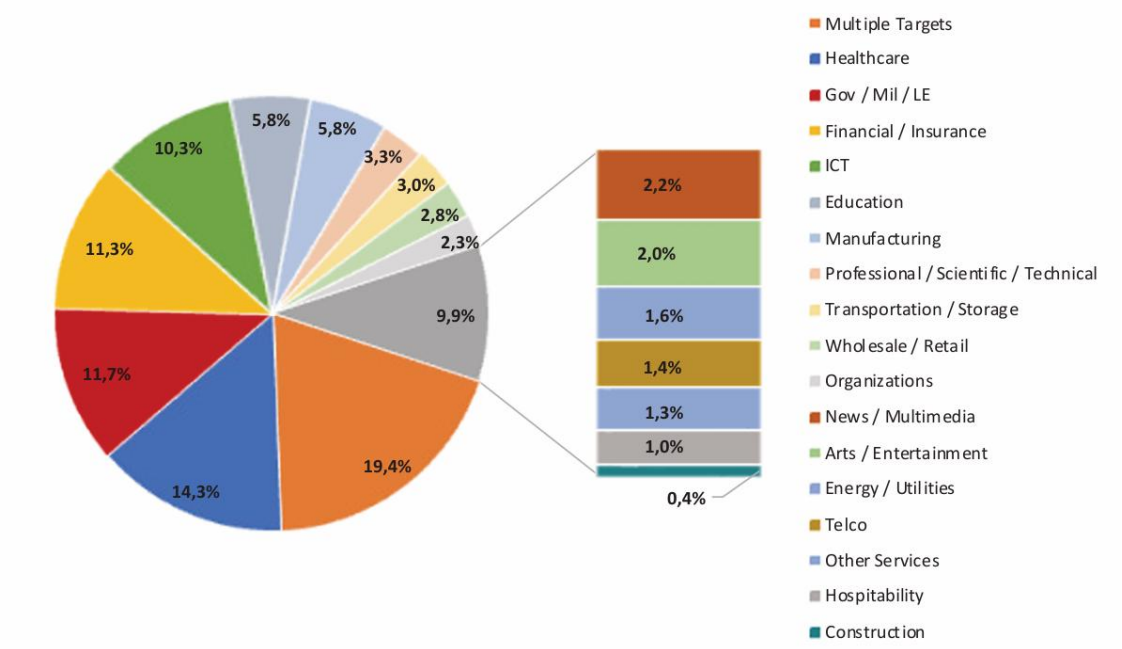

Figura 10: Istogramma dei settori più colpiti [5]

L'analisi dei numeri assoluti [Figura 11] tra il 2019 e il 2023 offre una visione più dettagliata su come lo scenario delle vittime sia cambiato in funzione dell'incremento complessivo degli attacchi. Sebbene l'incidenza percentuale degli attacchi verso bersagli multipli sia diminuita rispetto al 2022, il numero assoluto di attacchi è rimasto pressoché invariato (539 nel 2023 contro 541 nel 2022). Questo rende la categoria "Multiple Target" la più colpita per il secondo anno consecutivo. In parallelo, gli attacchi all'ambito governativo sono aumentati in modo significativo, passando da 301 a 325. I settori finanziario/assicurativo e sanitario hanno registrato una crescita consistente, con il settore sanitario che risulta il più colpito dopo la categoria dei bersagli multipli. Il settore ICT mantiene un numero stabile di incidenti, mentre gli attacchi verso i settori

manifatturiero, scientifico, trasporti/logistica e commercio all'ingrosso e al dettaglio mostrano una crescita significativa.

Si può constatare che praticamente tutti i settori industriali presentino un trend crescente di attacchi cyber e in particolare, se non si considerano i bersagli multipli, i tre settori più colpiti sono quello sanitario, militare, e finanziario.

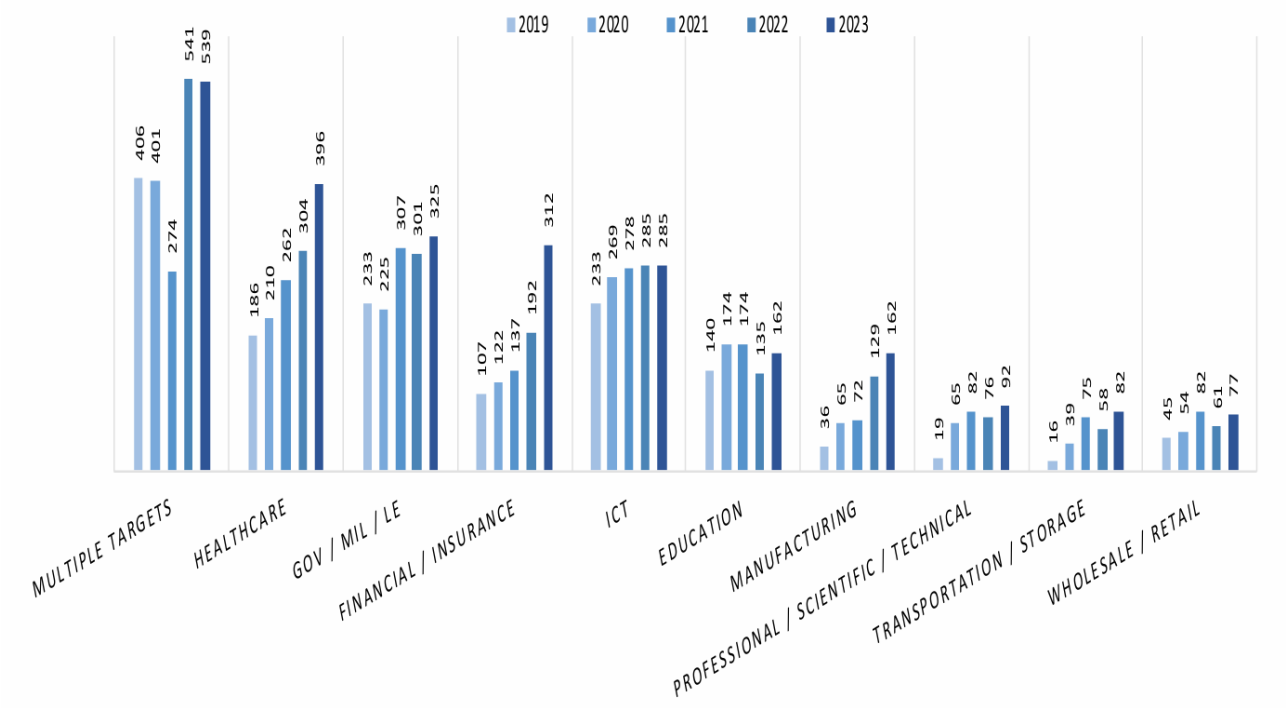

Figura 11: Attacchi 2019-2023 nei dieci settori più colpiti [5]

Tuttavia è importante valutare soprattutto la gravità di questi attacchi. L'analisi della criticità per settore colpito nel 2023 [Figura 12] e 2022 [Figura 13], per prima cosa, mostra che è in aumento la gravità per il settore medicale, da poco più del 20% nel 2022 al 40% nel 2023. Quelli finanziario, assicurativo e informatico sono aumentati del 10%. Il settore scientifico e professionale invece è aumentato del 20 %, arrivando al 40 % di severity. Restano invece costanti le percentuali verso bersagli multipli e scuole, mentre la severità delle conseguenze degli incidenti scendono nel settore governativo, seppur rimanendo abbastanza elevata.

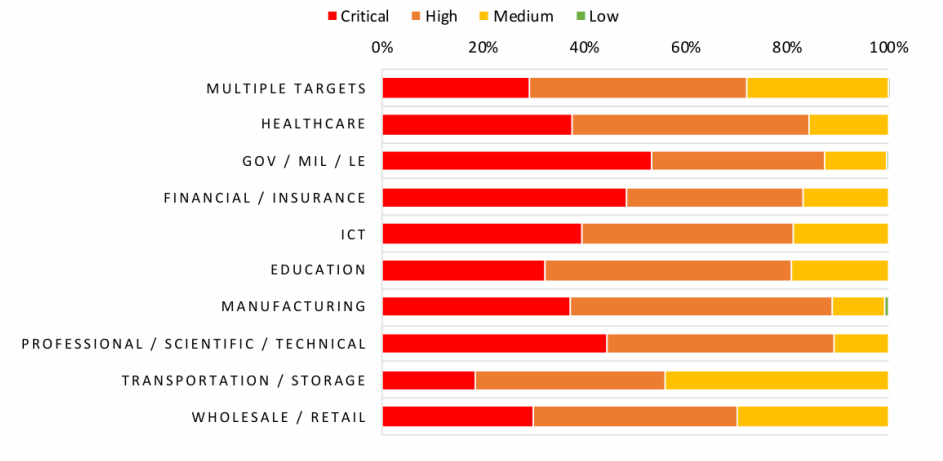

Figura 11: Severity per settori 2023[5]

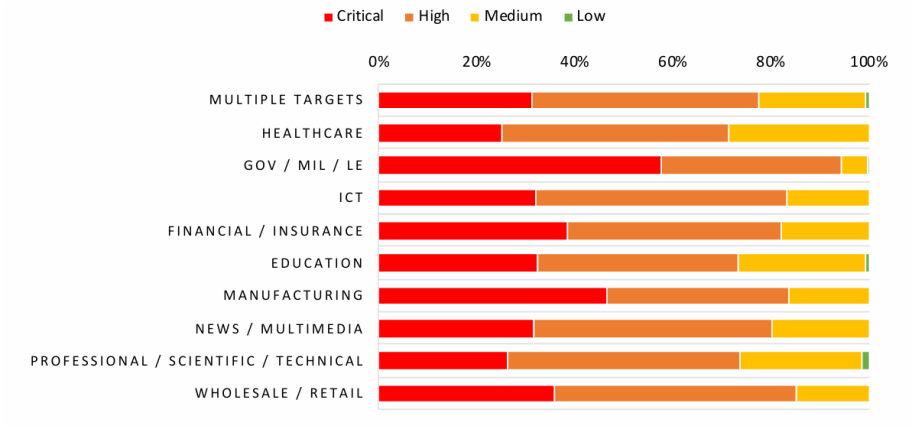

Figura 12: Severity per settori 2022[5]

2.2 Costi delle violazioni di sicurezza informatica e impatto sulla reputazione

Una volta appurato che i dati aziendali sono asset fondamentali per le imprese e che l'impatto degli attacchi informatici in qualsiasi settore, ogni anno, è sempre più critico, in questo capitolo si vuole cercare di quantificare economicamente l'impatto degli attacchi cibernetici. La perdita o il furto di dati sensibili, informazioni finanziarie, dati dei clienti, strategie di business, proprietà intellettuale e molto altro, può avere conseguenza devastanti per le imprese: la cybersecurity è fondamentale per proteggere questi beni preziosi, poiché una violazione di tali dati può provocare dei costi ingenti, danneggiare la reputazione delle aziende e persino causare la chiusura. Questi costi includono non solo le spese dirette per affrontare l'incidente, ma anche i costi indiretti, come la perdita di clienti e la diminuzione del valore azionario. Inoltre, le imprese potrebbero essere soggette a sanzioni legali e multe in caso di mancanza di adeguata protezione dei dati dei clienti. L'impatto sulla reputazione risulta altrettanto importante, perché un attacco informatico o il furto

di dati, può causare la fuga di clienti, compromettendo gravemente la loro fiducia verso l'organizzazione.

Secondo il Cost of a Data Breach Report 2024 di IBM[9] [7], uno studio che prende in esame 604 organizzazioni che hanno subito violazioni dei dati tra marzo 2023 e febbraio 2024, il costo medio globale di una violazione di dati è incrementato del 10% rispetto all'anno precedente [Figura 14], raggiungendo i 4,88 milioni di dollari, il più alto di sempre. In Italia il costo si aggira intorno a 4,7 milioni di euro, mentre negli Stati Uniti è quasi il doppio della media globale [Figura 15]. La crescita si spiega con l'incremento dei danni patrimoniali, derivanti da interruzioni del servizio (downtime) e perdita di clienti, e con il costo delle procedure post-attacco, come l'aumento di personale impiegato nell'help desk del servizio clienti e il pagamento di sanzioni più elevate per la violazione di normative. Nel complesso, questi costi ammontano a 2,8 milioni di dollari, ossia la cifra combinata di danni patrimoniali e costo di attività post-attacco più alta degli ultimi 6 anni.

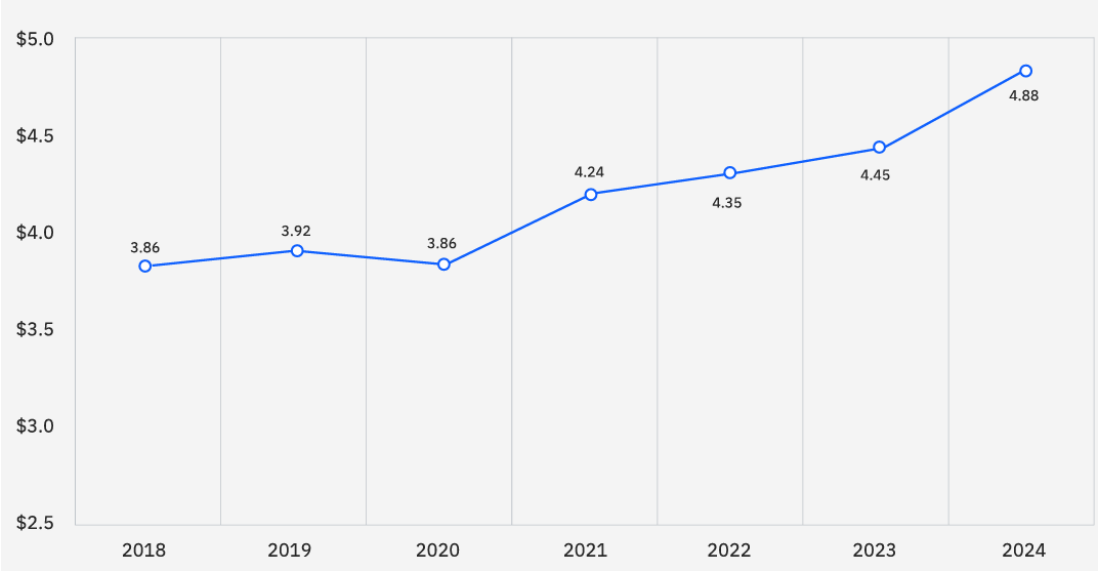

Figura 14: costo medio globale di un data breach [7]

[9] IBM è un fornitore leader a livello globale di cloud ibrido, AI e servizi di business integration

#	Cost change	2024	2023
1	↓	**United States** $9.36	**United States** $9.48
2	↑	**Middle East** $8.75	**Middle East** $8.07
3	↑	**Benelux** $5.90	**Canada** $5.13
4	↑	**Germany** $5.31	**Germany** $4.67
5	↑	**Italy** $4.73	**Japan** $4.52

Figura 15: top 5 paesi con impatto maggiore

Più della metà delle organizzazioni vittime di violazioni si trovano ad affrontare elevati livelli di carenza di personale addetto alla sicurezza informatica. Questo problema ha visto un aumento del 26,2% rispetto all'anno precedente, una situazione che ha portato a un aumento medio di 1,76 milioni di $ nei costi causati dalle violazioni. Il 35% dei casi ha coinvolto dati shadow[10], il che dimostra che l'immensa esplosione di dati sta rendendo più difficile il monitoraggio e la salvaguardia. Il furto di dati condivisi tramite cloud è correlato a un aumento del 16% nel costo di una violazione. Lo studio ha scoperto che l'archiviazione dei dati in ambienti diversi si è rivelata una tecnica diffusa, che rappresenta il 40% delle violazioni. Queste violazioni hanno anche richiesto più tempo per essere identificate e ostacolate.

Quasi la metà di tutte le violazioni coinvolgono informazioni di base dei dipendenti (PII) e dei clienti. Queste includono ad esempio codici identificativi (ID), e-mail, numeri di telefono e altre informazioni private. I record di proprietà intellettuale (IP) sono al secondo posto (43% delle violazioni). Il costo dei record IP è aumentato considerevolmente rispetto all'anno scorso, passando dai 156 dollari per record nello studio dell'anno scorso ai 173 dollari di quest'anno. Le violazioni che coinvolgono credenziali rubate o compromesse hanno richiesto più tempo per essere identificate e contenute (292 giorni è il tempo medio per identificare e limitare questo attacco informatico) rispetto a qualsiasi vettore di attacco. Anche attacchi simili che hanno coinvolto i dipendenti e l'accesso dei dipendenti hanno richiesto molto tempo per essere risolti. Ad esempio,

[10] Si definiscono Dati Shadow tutti quei contenuti caricati, salvati e condivisi in modo improprio su piattaforme di cloud storage.

gli attacchi di phishing sono durati in media 261 giorni, mentre gli attacchi di ingegneria sociale hanno richiesto in media 257 giorni [Figura 16].

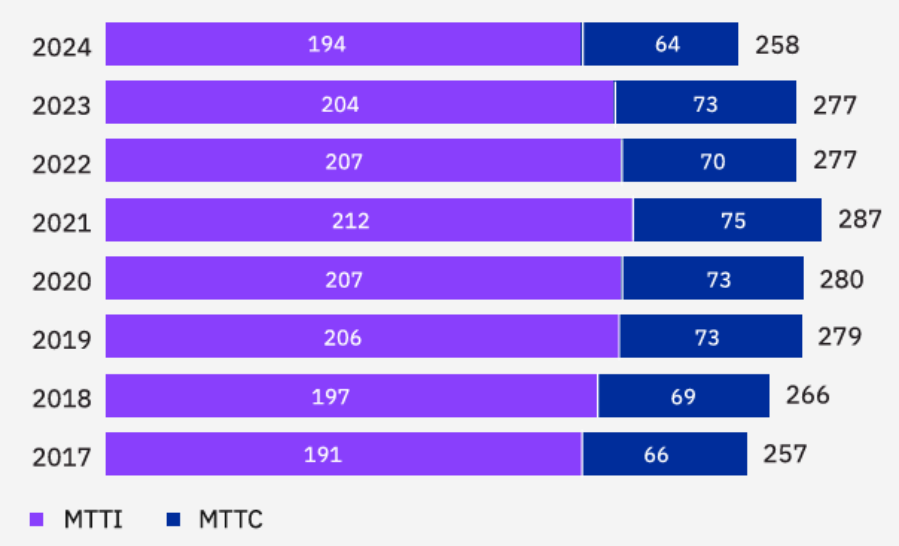

Figura 16: Tempo medio di identificazione e contenimento di un data breach [7]

Rispetto ad altri fattori, gli attacchi con "inserimento cyber" hanno comportato costi più alti, i quali hanno inciso in media 4,99 milioni di $. Le altre modalità di ingresso più costose sono la compromissione di e-mail aziendali, il phishing e il furto di password. La AI generativa ha incrementato la severità del phishing, perché rende più semplice, anche per chi non parla determinate lingue, produrre messaggi di phishing grammaticalmente corretti. Due terzi delle organizzazioni che hanno subito attacchi ransomware e hanno coinvolto le forze dell'ordine non hanno pagato il riscatto. Tali organizzazioni sono inoltre riuscite ad abbassare il costo degli attacchi con una media di quasi 1 milione di dollari, escludendo il costo dell'eventuale riscatto pagato. Il coinvolgimento delle forze dell'ordine ha inoltre contribuito a ridurre il tempo necessario per identificare e contenere le violazioni da 297 a 281 giorni.

Il settore industriale ha registrato il più alto aumento dei costi rispetto a tutti gli altri settori, con un aumento medio di 830.000 dollari per violazione rispetto allo scorso anno [Figura 17]. Questo aumento dei costi potrebbe indicare la necessità per le organizzazioni operanti nel settore industriale di prepararsi per una risposta più rapida, poiché le organizzazioni di questo settore sono altamente sensibili ai tempi di inattività operativa. Tuttavia, il tempo necessario per identificare e contenere una violazione dei dati presso queste organizzazioni è stato superiore alla media, pari a 199 giorni per l'identificazione e 73 giorni per il contenimento.

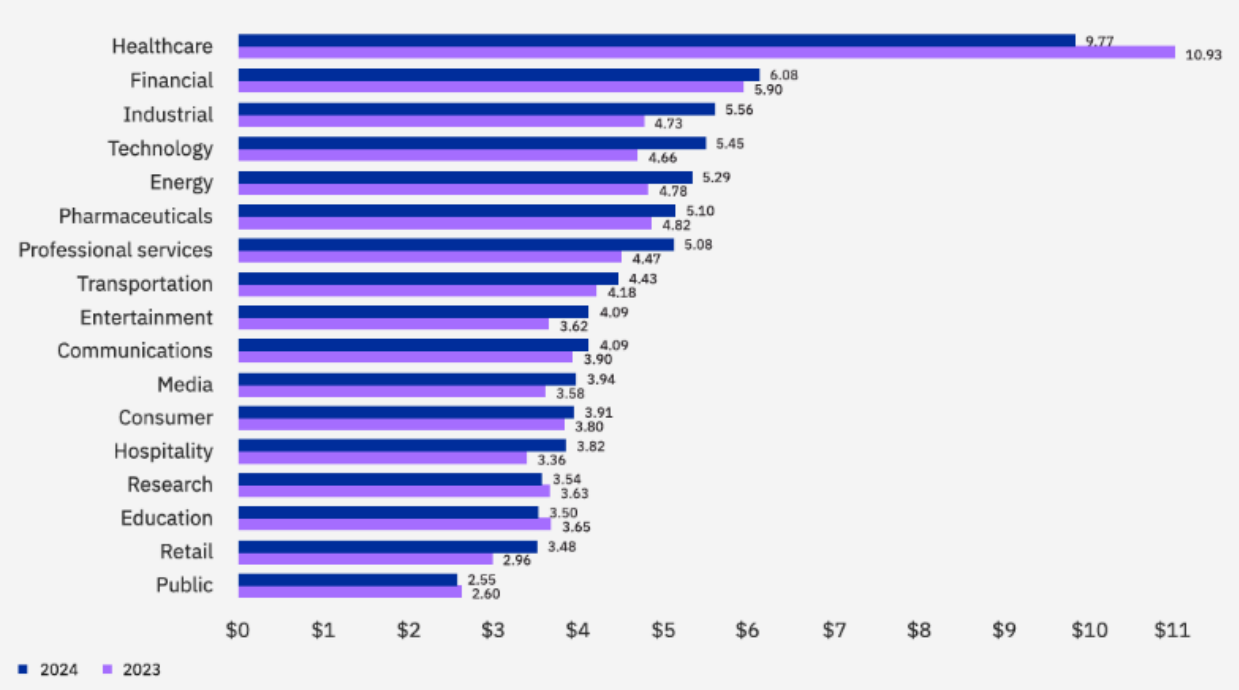

Figura 17: Costo medio data-breach per settore [7]

Possiamo constatare che il costo medio di una violazione informatica dipende da diverse variabili in gioco, ora cerchiamo di quantificarle e definirle:

I fattori aumentare il costa medio di una violazione informatica sono [Figura 18]:

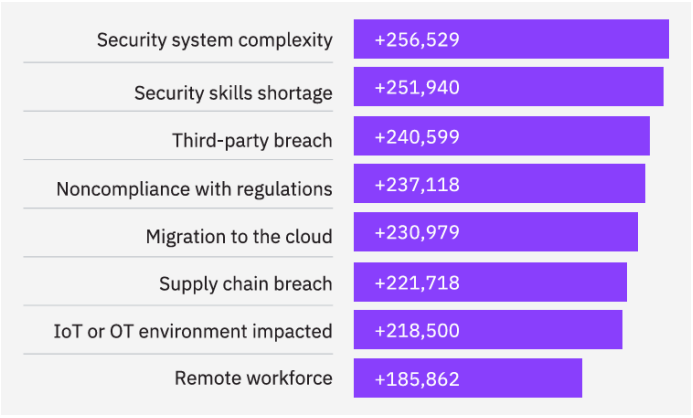

Figura 18: fattori che fanno incrementare il costo medio di un data-breach [7]

Si può notare che i tre fattori principali che fanno aumentare i costi delle violazioni in questa analisi sono stati la complessità del sistema di sicurezza, la carenza di competenze in materia di sicurezza e le violazioni di terze parti, che possono includere violazioni lungo la supply chain.

I fattori che fanno diminuire il costo medio di una violazione informatica sono [Figura 19]:

Figura 19: Fattori che fanno diminuire il costo medio di un data-breach [7]

La formazione dei dipendenti e l'uso di intelligenza artificiale e *machine learning*[11] sono stati i principali fattori che hanno mitigato i costi medi di violazione dei dati. La formazione dei dipendenti continua a essere un elemento essenziale nelle strategie di difesa informatica, in particolare per rilevare e fermare gli attacchi di phishing. Gli approfondimenti di intelligenza artificiale e apprendimento automatico sono al secondo posto.

Il seguente grafico mostra l'evoluzione della composizione del costo medio di un data breach [Figura 20]. I costi derivanti dalla perdita di business e dalla risposta post-violazione sono aumentati di quasi l'11% rispetto all'anno precedente, il che ha contribuito al significativo aumento dei costi complessivi delle violazioni. I costi di perdita di business includono la perdita di fatturato dovuta ai tempi di inattività del sistema e il costo dei clienti persi e il danno alla reputazione. I costi post-violazione includono la spesa per l'impostazione di call center e servizi di monitoraggio del credito per i clienti interessati e il pagamento di sanzioni normative.

[11] L'apprendimento automatico è una sottocategoria dell'intelligenza artificiale che raccoglie metodi sviluppati negli ultimi decenni del XX secolo in varie comunità scientifiche, sotto diversi nomi quali: statistica computazionale, riconoscimento di pattern, reti neurali artificiali, filtraggio adattivo, teoria dei sistemi dinamici, elaborazione delle immagini, data mining e algoritmi adattivi.

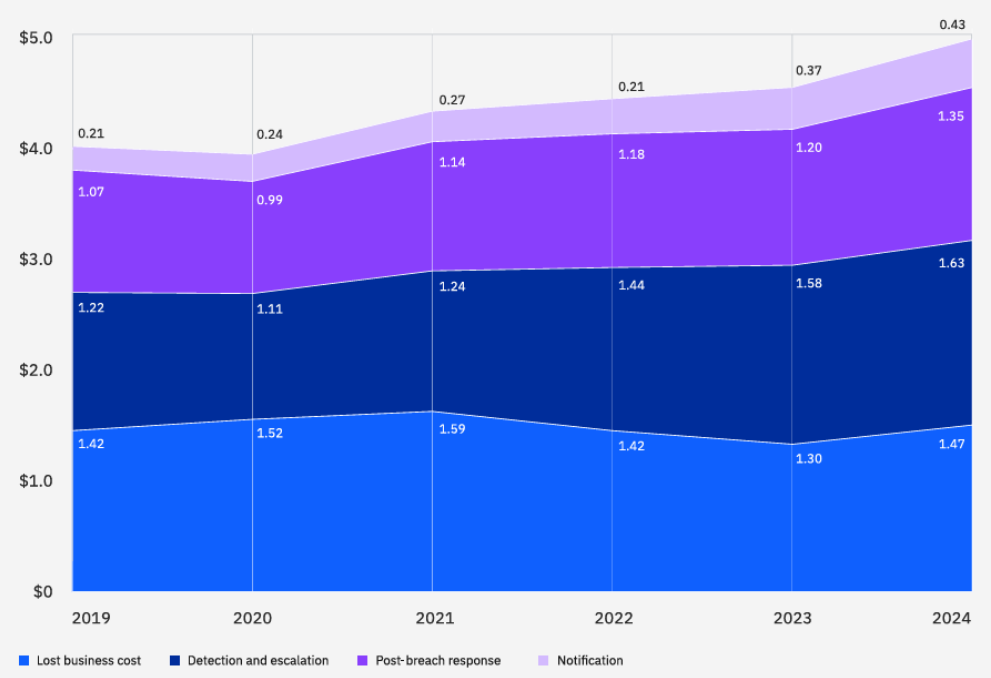

Figura 20: composizione average data breach cost [7]

Per ridurre il costo delle violazioni informatiche, quindi, sono consigliabili tre azioni principali:

- Conoscere l'archiviazione dei propri dati: la maggioranza delle aziende distribuisce i dati su più server come cloud privati e pubblici. Tuttavia, molte organizzazioni hanno un monitoraggio dei dati non completo o in tempo reale, accorgendosi troppo tardi di quali dati siano stati violati e quanto siano ancora sensibili o riservati. Questi ritardi possono complicare la risposta e aumentare il costo di una violazione. I team addetti alla sicurezza dovrebbero garantire una visibilità completa su tutti questi ambienti, in modo da poter monitorare e proteggere continuamente i dati indipendentemente da dove risiedono. I team di sicurezza devono prestare particolare attenzione agli ambienti ibridi e ai cloud pubblici. Un quarto dei data breach ha visto coinvolti dati archiviati in diversi ambienti e, soprattutto quando questi erano stati memorizzati nel cloud pubblico, hanno registrato il costo medio più impattante, pari a 5,17 M$. È fondamentale che i team di sicurezza acquisiscano una comprensione più approfondita dei rischi e dei controlli specifici per ciascun cloud service utilizzato. La gestione dei dati tra diversi ambienti viene ulteriormente complicata dall'impatto dei dati non gestiti. Oltre un terzo delle violazioni dei dati riguarda i dati shadow. I team di sicurezza devono ora presumere che la propria organizzazione disponga di origini dati non gestite. I dati non crittografati, inclusi i dati dei workload AI, aggravano ulteriormente il rischio. La strategia di crittografia dei dati deve considerare le tipologie di dati, il loro utilizzo e dove risiedono per ridurre il rischio in caso di violazione.

- Rafforzare la strategia di prevenzione con AI e automazione: Due organizzazioni su tre coinvolte nello studio hanno dichiarato di implementare l'AI e il machine learning nel proprio centro per le operazioni di sicurezza informatica, con un incremento del 10% rispetto all'anno precedente. Attraverso un'implementazione ampia dell'AI nei processi di prevenzione (gestione dei confini di attacco e gestione del livello di sicurezza), le organizzazioni hanno registrato in media una riduzione di 2,2 milioni di dollari nei costi derivanti dalle violazioni rispetto a chi non utilizza questo strumento. Si tratta del risparmio sui costi più importante tra quelli rilevati da IBM. L'adozione di modelli di AI in tutte le business unit aziendali e l'uso sempre più diffuso dell'Internet of Things (IoT) stanno espandendo l'area di attacco esercitando pressione sul personale addetto alla sicurezza IT. Le organizzazioni che hanno sfruttato l'AI e l'automazione nelle *operations* di prevenzione cyber hanno riscontrato rendimenti maggiori dai propri investimenti in AI rispetto ad altre tre divisioni di sicurezza: rilevazione, analisi ed esecuzione. Tali organizzazioni hanno risparmiato in media 2,22 M$ rispetto alle organizzazioni che non hanno sfruttato l'AI nelle tecnologie di prevenzione [Figura 21].

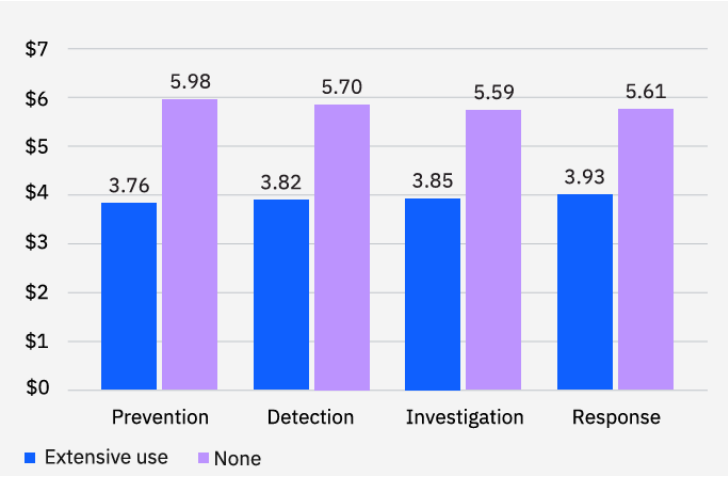

Figura 21: Risparmio sul costo di un data-breach quando si implementa AI nelle security operations [7]

- Migliorare l'educazione sulla risposta al rischio cyber: la modalità con cui un'organizzazione reagisce e comunica durante e successivamente una violazione (con la governance aziendale, le autorità di regolamentazione e i clienti) è un aspetto fondamentale. Tre quarti dell'aumento dei costi medi è stato determinato dal costo del lucro cessante, comprendente *downtime*, perdita di clienti e ordini, e acquisizione di nuovi clienti. Sono state incluse anche le attività di risposta post-violazione, come la creazione di un centro assistenza per i clienti e il pagamento di more per non conformità alla norma. Risulta fondamentale quindi investire nella gestione della risposta post-violazione perché permette

di ridurre i costi di una data breach. Per diminuire l'impatto sui costi, tutelare i propri clienti e salvaguardare la continuità operativa è quindi necessario che le organizzazioni integrino le funzionalità di risposta tecnica con il proprio *business plan*. Integrare questi aspetti nella *governance* e adottare decisioni in anticipo può aiutare la gestione di gravi interruzioni dei processi e a semplificare le azioni che andranno a proteggere l'azienda in caso di attacco.

2.3 Analisi degli investimenti in cybersecurity

Parallelamente all'aumento degli attacchi informatici, anche gli investimenti nella sicurezza digitale stanno registrando una crescita costante negli ultimi anni per contrastare le minacce emergenti [Figura 22]. Il mercato globale della cybersecurity, valutato 222 miliardi di dollari nel 2022, è previsto in espansione fino a 657 miliardi di dollari entro il 2030, con un tasso di crescita annuale del 12,8% nel periodo 2022-2030 [8].

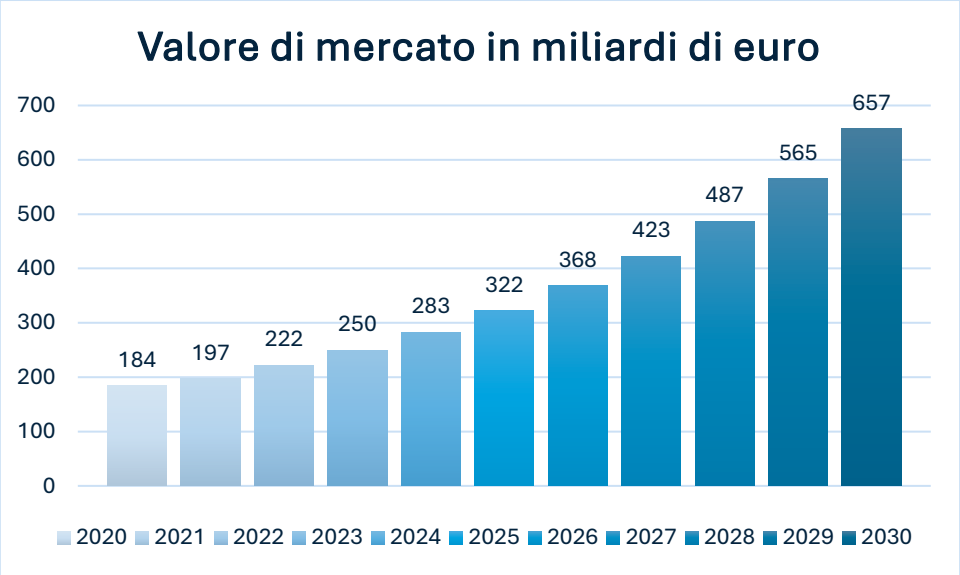

Figura 22: Mercato globale cybersecurity

Il mercato globale della sicurezza informatica mostra quindi una crescita costante. Questa tendenza è evidente anche nell'aumento della spesa globale, che è passata da 101,5 B$ nel 2017 a 169 B$ nel 2022. Le previsioni indicano un'ulteriore espansione nei prossimi anni, con una spesa mondiale per la cybersecurity che, nel 2024, sarà più che doppia rispetto al 2017 [Figura 23].

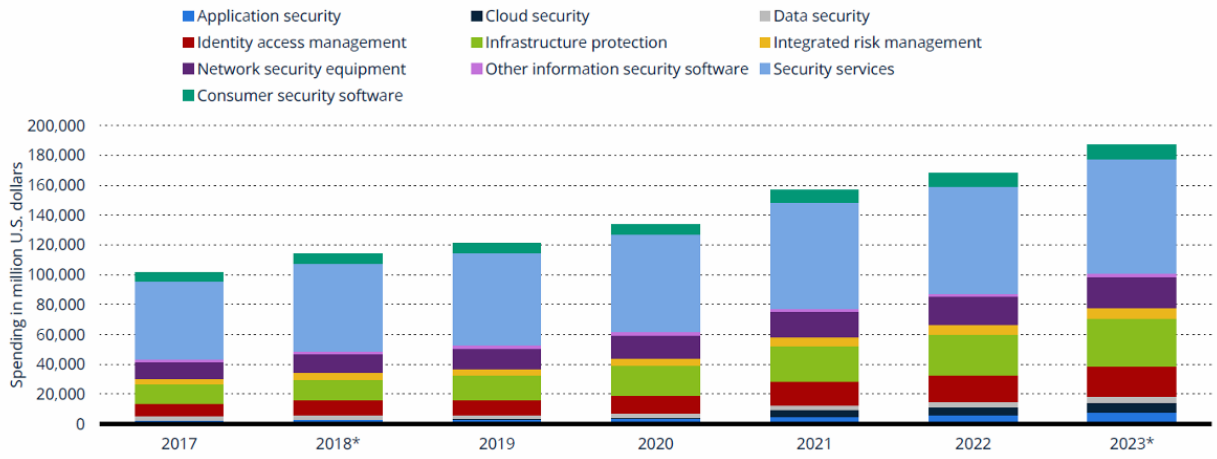

Figura 23: spesa mondiale in cybersecurity

Secondo l'analisi di Gartner, i servizi di sicurezza, la protezione delle infrastrutture e le apparecchiature per la sicurezza delle reti hanno rappresentato la principale priorità per le organizzazioni. Nel 2023, l'area più critica della cybersecurity è risultata essere la sicurezza dei dati, seguita dalla privacy e dalle statistiche di cybersecurity [9]. Ne deriva che la sicurezza dei dati e delle applicazioni siano considerate nuove priorità e sanciscono chiaramente come le aziende stiano ridefinendo le proprie strategie di sicurezza informatica e i propri investimenti. A eccezione di queste due nuove aree, l'attenzione verso gli altri aspetti della cybersecurity sembra in calo. Una categoria da monitorare con attenzione è l'analisi del rischio, essenziale come guida per prendere decisioni sugli investimenti e sull'allocazione del budget [Figura 24] [10].

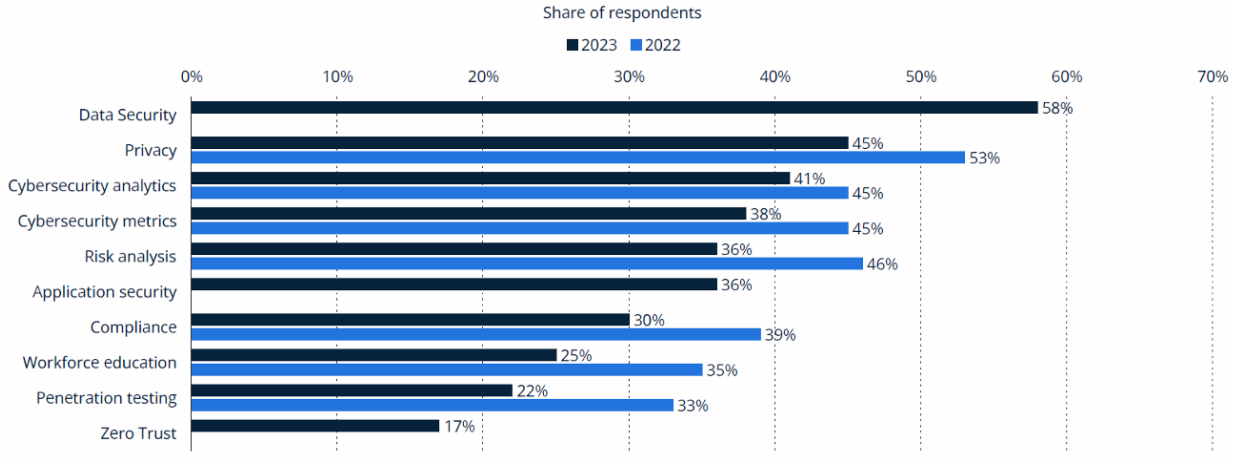

Figura 24:aree più critiche

Con la crescente consapevolezza delle minacce informatiche e dell'importanza di implementare sistemi di sicurezza adeguati, aumenta anche il numero di professionisti nel settore della cybersecurity. Le figure con hard skills per proteggere sistemi, infrastrutture di reti da attacchi informatici sono tra le più richieste nel mercato del lavoro attuale, con una domanda che cresce più

velocemente rispetto all'offerta disponibile. A livello globale, nel 2022 il numero di professionisti della cybersecurity ha raggiunto i 4,6 milioni, in aumento rispetto ai 4,1 milioni del 2021. La maggior parte di questi esperti si trova negli Stati Uniti, dove nel 2022 si stimavano oltre 1,2 milioni di professionisti. L'Italia, invece, registra un ritardo rispetto alla media mondiale [Figura 25].

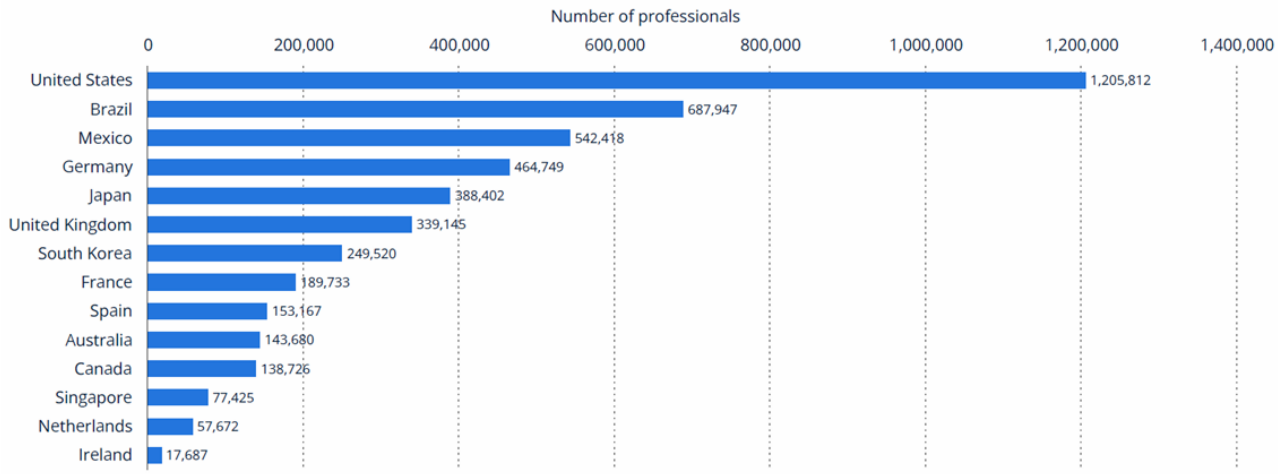

Figura 25: professionisti in cybersecurity

Tra il 2016 e il 2023, il mercato della cybersecurity in Italia è aumentato, passando da 976 milioni di euro a 1,855 miliardi di euro, come mostrato in [Figura 26] [11].

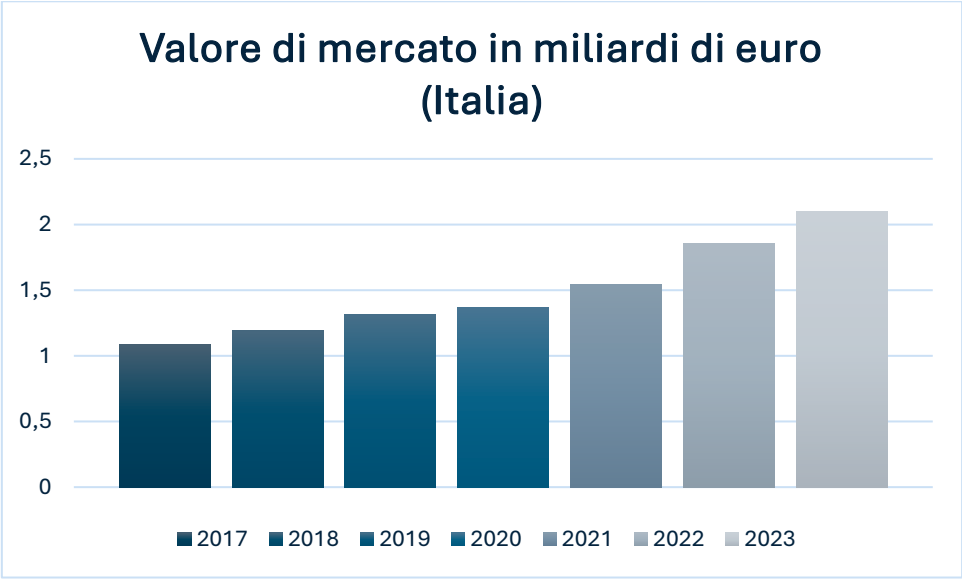

Figura 26: mercato della cybersecurity in Italia

Nel 2022, l'Italia ha registrato, in termini percentuali, il più alto tasso di investimenti in cybersecurity dell'ultimo quinquennio, con una spesa totale di 1,855 miliardi di euro, segnando un aumento del 18% rispetto al 2021 [Figura 27]. Questo rialzo è il risultato diretto dell'aumento del numero di attacchi rilevati, come analizzato nel capitolo precedente.

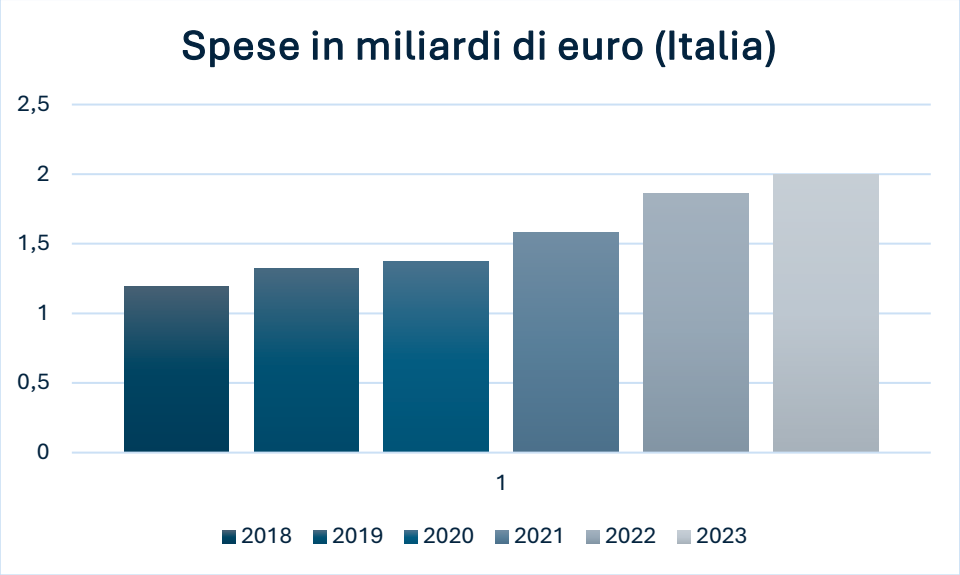

Figura 27: investimenti in cybersecurity in Italia

Tuttavia, questo non è sufficiente per collocare l'Italia in una posizione competitiva tra le principali economie avanzate del G7. Infatti, l'Italia occupa l'ultima posizione nel rapporto tra investimenti in cybersecurity e PIL. Al vertice della classifica si trovano gli Stati Uniti e il Regno Unito, con una quota dello 0,31%, seguiti dagli altri paesi con valori compresi tra lo 0,22% e lo 0,18%, mentre l'Italia si ferma allo 0,1% [Figura 28] [12]. Rispetto agli anni precedenti, si è registrato un lieve aumento di qualche decimo di punto.

	Investimenti in C.S./ PIL
Media globale	0,20%
USA	0,31%
UK	0,31%
Giappone	0,22%
Canada	0,20%
Francia	0,19%
Germania	0,18%
Italia	0,10%

Figura 28: Rapporto tra investimenti in c.s. e PIL

Un dato che suggerisce che l'Italia stia iniziando a muoversi nella giusta direzione e a riconoscere l'importanza della cybersecurity è il risultato di un sondaggio del 2022, secondo cui il 61% delle

grandi aziende italiane ha dichiarato di aver aumentato il proprio budget per la sicurezza informatica. Solo il 3% dei partecipanti ha riferito una riduzione di tale finanziamento [Figura 29].

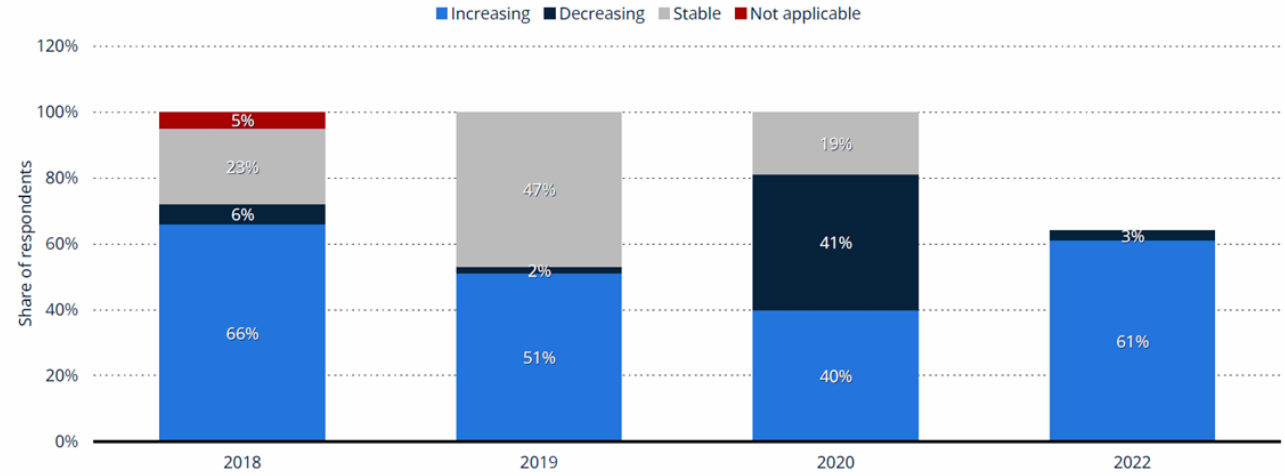

Figura 29: percentuale di aziende che incrementano il budget in c.s.

Da recenti studi emerge che tre quarti delle imprese italiane con almeno dieci dipendenti utilizza più di tre misure di sicurezza informatica [Figura 30]. Questo dato è il linea con la media europea che si attesta al 74%. Risulta evidente che le aziende di piccole dimensioni adottino misure di sicurezza meno forti [Figura 31], ad esempio sono manchevoli di strumenti quali l'autenticazione con password forte e il back-up dei dati. Si riscontra ancora molto limitata invece la diffusione di misure avanzate di protezione, come l'utilizzo della crittografia per dati, i metodi biometrici per l'accesso, le analisi di valutazione del rischio e l'esecuzione ciclica di test.

L'aumento degli accessi alla rete da remoto, ad esempio tramite il lavoro in smart working, espone le imprese a rischi sempre più crescenti. Si sono verificate pericolose intrusioni dall'esterno che hanno causato downtime dei servizi e fughe di dati. Statistiche ISTAT del 2022 affermano che il 15,7% delle imprese con almeno dieci addetti e il 33,1% delle imprese con almeno 250 addetti hanno dichiarato di aver subito almeno uno di questi problemi. Quasi la metà delle imprese dispongono di documenti relativi a misure e procedure di sicurezza informatica. Di queste imprese l'85,7% ha aggiornato tali documenti negli ultimi due anni. Inoltre, indicativo della scarsa percezione del rischio cyber, solo il 16,4% delle imprese hanno dichiarato di essersi assicurate contro incidenti informatici [13]. Nel capitolo successivo verrà analizzata nello specifico questa preoccupante tendenza in Italia.

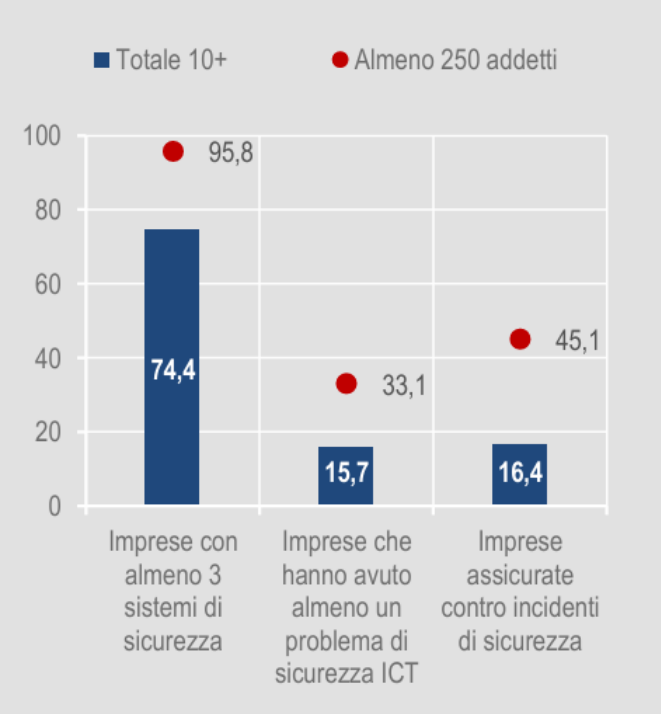

Figura 30: % in base alla dimensione aziendale in Italia [13]

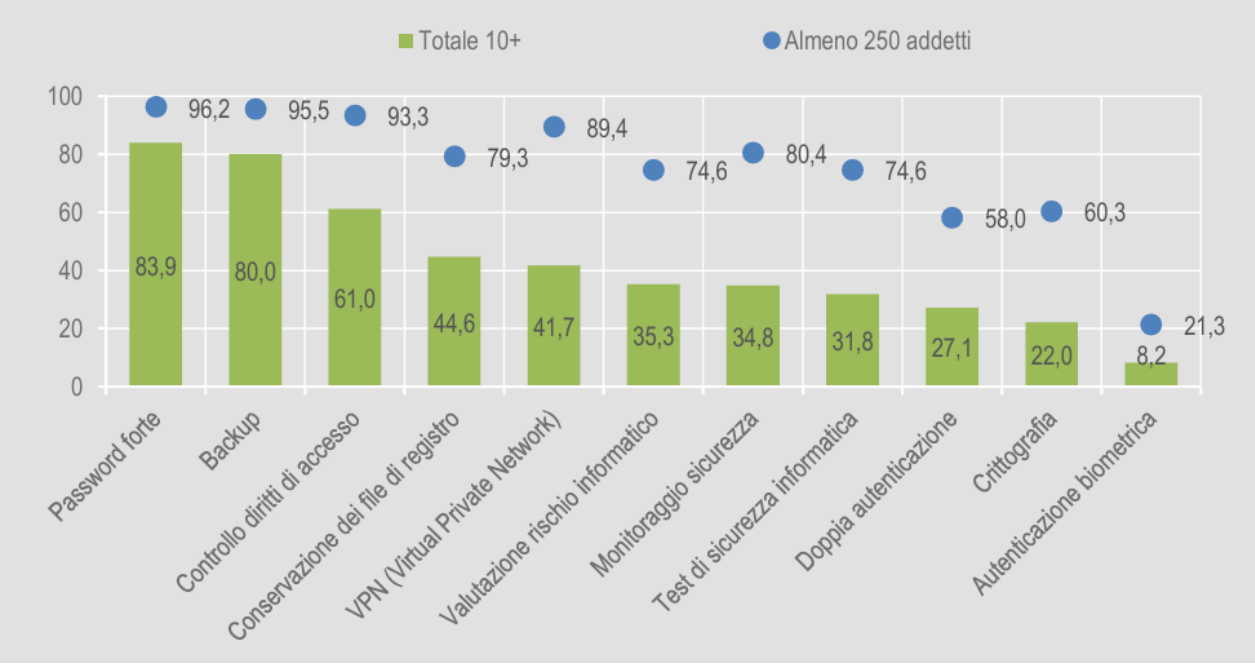

Figura 31: Adozione degli elementi di c.s. in base alle dimensioni aziendali [13]

Questa panoramica degli ultimi anni, caratterizzati da investimenti senza precedenti nel settore della cybersecurity, evidenzia la crescente consapevolezza riguardo alle minacce informatiche nel contesto attuale. Con l'espansione delle attività digitali, la salvaguardia dei dati sensibili è diventata un punto d'interesse fondamentale per imprese, enti governativi e utenti privati. Gli attacchi informatici, sempre più complessi e mirati, richiedono un costante affinamento della protezione

digitale, orientando le organizzazioni a puntare su tecnologie innovative, formazione e la costruzione di strategie di sicurezza corretti ed efficaci. Questi *capex* non solo proteggono da possibili danni economici e reputazionali, ma sono anche fondamentali per incidere sulla fiducia del pubblico e garantire l'integrità di tutte le *operations*. Infine, l'avvento di tecnologie emergenti come l'intelligenza artificiale e l'Internet delle cose ha portato nuove sfide e opportunità nel campo della cybersecurity, rendendo indispensabili investimenti continui e mirati per rimanere sempre un passo avanti rispetto agli attaccanti digitali. In questo scenario, l'innovazione e l'impegno costante nella sicurezza informatica non solo proteggono dalle minacce, ma rappresentano anche un impulso per lo sviluppo sostenibile e per rafforzare la fiducia nell'ecosistema digitale globale.

3. Il fattore umano e l'importanza della sensibilizzazione sulla cybersecurity

Solo da pochi anni le aziende si sono effettivamente rese conto dell'importanza della sicurezza informatica. Una tendenza comune, che ancora oggi risulta diffusa, è il fatto che si creda che queste questioni siano da destinare solamente ai reparti IT delle organizzazioni. Sicuramente queste figure sono le più preparate dal punto di vista tecnico su tale materia, tuttavia, facendo così, non si riuscirà mai a costruire una strategia comune per mitigare il rischio informatico. Come abbiamo potuto apprendere dal capitolo precedente, la maggior parte degli attacchi informatici riusciti con successo sono stati scaturiti da errori umani e dallo sfruttamento di vulnerabilità dei sistemi. In questo senso, gioca un ruolo fondamentale la sensibilizzazione e l'educazione informatica, per tutti i livelli di dipendenti, fino ad arrivare alle figure dell'alto management. La situazione attuale afferma che la maggior parte dei dirigenti d'azienda ignori completamente i protocolli di sicurezza IT e i gravissimi impatti che potenzialmente possono essere generati. Inoltre, soprattutto per le aziende in Italia, recenti studi hanno registrato una comune avversione riguardo la capacità di investire in protezione e prevenzione in cybersecurity.

3.1 L'esigenza di sviluppare la cybersecurity awareness

Il futuro della cybersecurity si sta delineando con sempre maggiore chiarezza nel panorama mondiale, in quanto le organizzazioni iniziano a guardare oltre le minacce, piuttosto verso i potenziali impatti positivi che possono ottenere integrando in modo profondo il pensiero e le azioni relative alla sicurezza informatica nelle loro attività. Alcuni dati significativi riguardano la sempre maggiore importanza che le tematiche relative alla cybersecurity stanno assumendo in azienda: secondo recenti studi condotti da varie aziende di consulenza il 70% delle organizzazioni sentite ha riferito che le attività di individuazione delle minacce sono ordinarie durante le riunioni del proprio consiglio di amministrazione su base mensile o trimestrale. Infatti, la grande maggioranza degli intervistati ha individuato un forte legame tra il cyber e l'impatto sul business, con l'86% che ha dichiarato che le iniziative cyber hanno contribuito in modo significativo e positivo ad almeno una priorità aziendale. In base a questo dato, la maggior parte delle organizzazioni sta cercando di sfruttare questa proposta di valore, con il 58% che prevede di aumentare i propri investimenti informatici nel prossimo anno. Altri dati confermano ulteriormente questa tendenza in crescita, riguardante il grado di formazione e diffusione dei principi di cybersecurity:

- Entro il 2028, il 65% delle organizzazioni si è prefissata l'obiettivo di utilizzare il profilo della sicurezza informatica come elemento chiave per valutare operazioni e rapporti

commerciali seguendo una tendenza che ha iniziato ad affermarsi nel 2020, quando le aziende più sensibili all'argomento hanno iniziato a misurare il costo dei data breach.

- Nel 2028, quattro aziende su dieci avrà una sezione dei cda [12] dedicata alla cybersecurity.
- Entro il 2028, tre quarti degli amministratori delegati svilupperà una cultura aziendale di resilienza per proteggere la propria organizzazione da cyberattacchi.

Le aziende avranno quindi una responsabilità sempre più presente nella sensibilizzazione, ma, nonostante ciò, la responsabilità sarà dell'utente finale o del lavoratore, il quale dovrà imparare a utilizzare consapevolmente qualsiasi *devices*, rispettare norme di un corretto utilizzo e proteggere i propri dati sia al lavoro sia nella vita privata. La situazione paventata per il 2024 non era delle migliori. Secondo i principali player di mercato si potrebbe creare una voragine tra le aziende attente al cyberspace, in grado di formare bene i dipendenti e dotarsi di tecnologie adeguate, e le altre realtà, che potrebbero diventare facile preda dei cyber criminali. Proprio perché gli attacchi e truffe si basano sempre più spesso su tecniche che sfruttano le debolezze del fattore umano, sono in grande ascesa tutte le iniziative mirate ad aumentare la consapevolezza e la formazione sul tema, necessaria anche da un punto di vista normativo con il costante aumento della pressione di compliance sui temi della cyber security, si pensi ad esempio all'impatto di NIS/NIS 2, oltre ovviamente al GDPR[13], i quali verranno approfonditi nel capitolo quattro. Per tutti questi motivi Enisa[14] stanno definendo la necessità di prevedere l'inserimento di figure specializzate e piani di formazione. È divenuta ormai imprescindibile, infatti, la necessità di dotarsi di piani di formazione strutturata per gestire la vulnerabilità derivante dal fattore umano con l'attivazione di iniziative di sensibilizzazione rivolte ai possibili impatti diretti e concreti cyber delle attività dei dipendenti, come confermano i seguenti dati [Figura 32]: le grandi organizzazioni in Italia si sono rese conto della necessità di introdurre iniziative di formazione (siamo al 99%), tra questi alcuni hanno un programma strutturato (80%), solo l'1% dichiara che non sono previste [14].

[12] Consiglio di amministrazione
[13] Il regolamento generale sulla protezione dei dati in sigla RGPD (o GDPR in inglese General Data Protection Regulation)
[14] Agenzia dell'Unione europea per la cibersicurezza

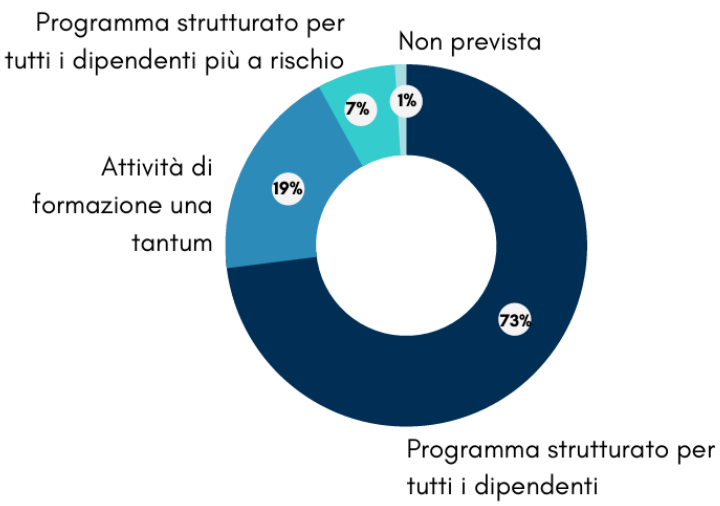

Figura 32: Risultati di un questionario rivolto alle aziende italiane [14]

Le aziende cercano di dare un'impronta concreta a tali iniziative di formazione, ad esempio cercando di ricreare uno scenario di attacco di phishing e vedere la risposta dell'utente aziendale, oppure attraverso lezioni o eventi periodici dedicati interattivi per favorire il confronto sul tema e capire come la propria attività quotidiana potrebbe potenzialmente esporre l'azienda a un rischio cyber. È fondamentale, infatti, non solo che tali iniziative vengano implementate, ma che siano soprattutto efficaci e valutabili attraverso specifiche metriche. Questo richiede una stretta collaborazione tra diverse funzioni aziendali, in modo che, un tema di tale importanza, non venga affidato solo alle risorse umane, ma a tutte le risorse tecniche e informatiche.

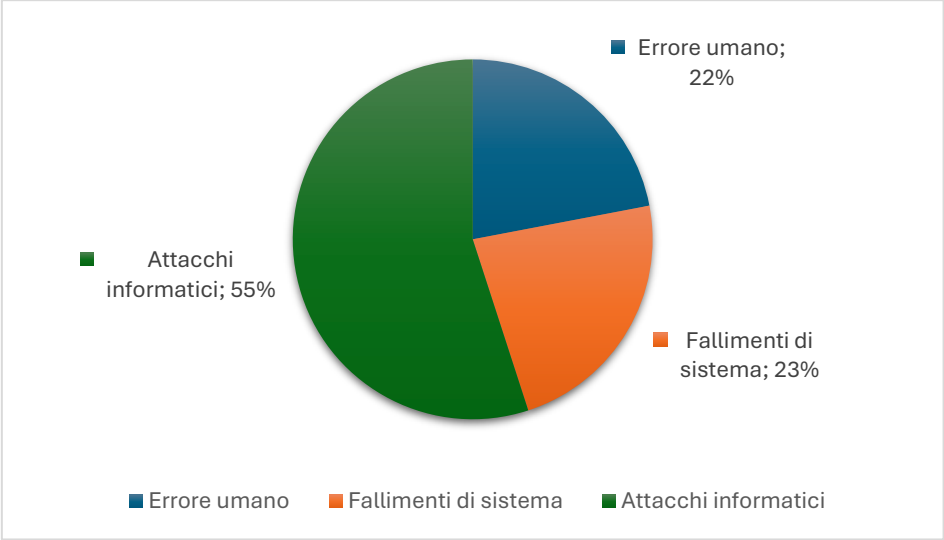

Figura 33: Istogramma sulle cause di attacchi informatici [7]

Se si considera il grafico soprastante [Figura 33], si può vedere che una significativa percentuale di incidenti in sicurezza informatica deriva da qualche forma di errore umano. Un esempio di

attacco informatico scaturito da una leggerezza di un utente è quello che nell'estate 2021 ha colpito un centro pubblico regionale di elaborazione di dati legati all'emergenza pandemica. Nello specifico si è trattato di un attacco Ransomware, insinuatosi in un dispositivo di un dipendente che lavorava a distanza, tramite una connessione internet non sicura. Questo attacco causò il blocco di diverse infrasttrutture e sistemi, tra cui il portale del sistema sanitario locale, e un'ingente fuga di dati e i relativi costi che ne derivano. Questo episodio mette in mostra come in pochi minuti queste tecnologie possano mettere a repentaglio diversi sistemi, organizzazioni e addirittura interi stati. Per cercare di arginare questo problema bisogna agire su più ambiti contemporaneamente. Per prima cosa investire maggiormente in protezione dei sistemi dal punto di vista tecnologico. In secondo luogo dal punto di vista legislativo, poiché solamente con un quadro normativo il più chiaro e completo possibile si possono defire gli stardard di sicurezza da rispettare. Per ultimo, ma non per importanza, incentivare l'uso consapevole dei dispositivi e dei rischi legati alla sicurezza informatica.

Nell'esempio citato precedentemente e in generale nella maggior parte dei casi, l'esito positivo di un attacco è determinato dall'azione inconsapevole delle persone. Alcuni studi affermano addirittura che quasi il 97% degli attacchi sia dovuto a questa causa, invece solo una piccola parte maginale è dovuta ad aspetti più tecnici. Questo accade perché il più delle volte le persone agiscono inconsapevolemente e non hanno alcuna percezione dei rischi che possono incorrere sulla rete.

Come si nota da un sondaggio condotto da Kaspersky Lab e B2B International, oltre il 50% delle aziende vede nei propri dipendenti una delle principali vulnerabilità in ambito di sicurezza informatica. Si afferma che questa criticità deriva dalla scarsa conoscenza delle tematiche in ambito di cybersecurity, criticità che può compromettere l'intera strategia di protezione aziendale.

Le principali preoccupazioni riguardano la condivisione di dati tramite dispositivi mobili, il rischio per la perdita fisica di tali dispositivi e l'uso improprio delle risorse informatiche del personale. L'incidenza di questo fenomeno è statisticamente diversa per dimensioni aziendali: le microimprese tendono a percepirsi più esposte rispetto alle grandi organizzazioni, probabilmente a causa di policy più rilassate e di una formazione meno strutturata sui temi della sicurezza rispetto a grandi aziende che riescono a gestire in modo migliore queste minacce grazie all'ausilio di protocolli di sicurezza più rigorosi. Cresce il numero di incidenti dovuti a errori umani in micro-imprese: il tasso d'incidenti provocati da distrazioni, impreparazione e ingenuità dei lavoratori, tanto in ambito piccoli uffici quanto industriali, è passato dal 25% al 32 %. Inoltre, tra il 44% e il

48% delle aziende conferma che si trova vulnerabile di fianco al pericolo della poca informazione dei suoi dipendenti.

Tabella 1: impatto finanziario medio delle azioni dei dipendenti

Tipologia di organizzazione	Impatto finanziario medio di azioni inappropriate di dipendenti
Piccole e medie imprese (PMI)	-Condivisione impropria dei dati: $ 88.000 -Smarrimento dei dispositivi mobili che espone l'organizzazione a rischi: $ 99.000 -Smarrimento di dispositivi o supporti contenenti dati: $ 81.000 -Utilizzo inadatto delle risorse informatiche da parte dei dipendenti aziendali: $ 68.000
Grandi Imprese	-Incidenti che coinvolgono dispositivi IoT: $ 1,6 milioni -Smarrimento di dispositivi o supporti contenenti dati: $ 1,1 milioni - Utilizzo inadatto delle risorse informatiche da parte dei dipendenti aziendali: $ 581.000 -Condivisione inappropriata dei dati tramite dispositivi mobili: $ 464.000

Abbiamo quindi spiegato come le persone e i loro comportamenti siano il principale fattore scatenante degli attacchi informatici.
Come si può leggere dall report "Cybersecurity in Smart Factories" di Capgemini[15], molte strutture aziendali presentano una preparazione carente in termini di consapevolezza, governance, protezione, rilevamento e resilienza [Figura 34] [16].

[15] Multinazionale di servizi di consulenza

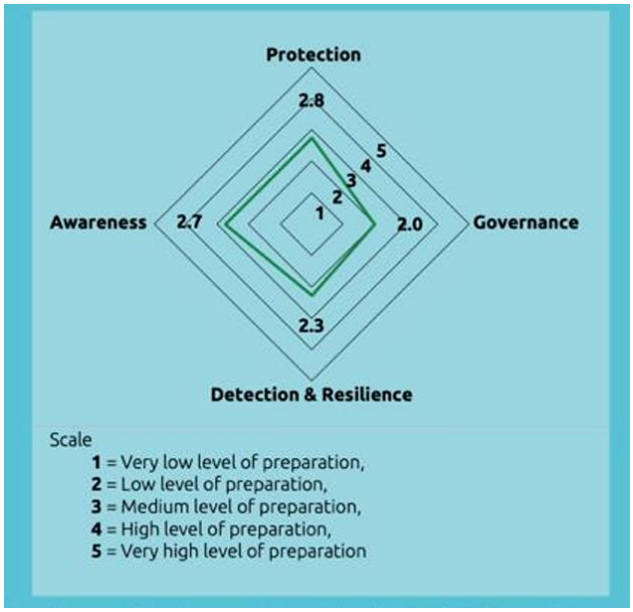

Figura 34: Analisi quantitativa condotta da Capgemini

L'analisi condotta da Capgemini19 illustra come la preparazione media delle organizzazioni in materia di cybersecurity sia ancora insufficiente, con un punteggio di 2,8 su 5. Nonostante alcuni miglioramenti in aree specifiche, la sicurezza complessiva presenta criticità, in particolare nella governance della cybersecurity, dove molti sistemi risultano poco integrati. Si rileva infatti che il 47% dei produttori non considera la sicurezza informatica una priorità per il management, mentre per il 44% è superfluo investire ulteriormente nella protezione dei processi produttivi, portando così a un punteggio medio di appena 2,0 in questo settore.

Anche la consapevolezza e la capacità di rilevare anomalie mostrano valori bassi, rispettivamente 2,4 e 2,0. Questo è indicativo di una preparazione inadeguata e di una limitata capacità di risposta alle minacce informatiche. In questo contesto emerge l'importanza fondamentale della formazione dei dipendenti. Questi, infatti, se adeguatamente formati, possono essere un punto di forza nella strategia di difesa, e prevenire in modo più efficace il riconoscimento degli attacchi di phishing.

Istruire i dipendenti ad una formazione dettagliata potrebbe sembrare solo un costo apparentemente superfluo ma è essenziale considerarlo come un vero investimento: è stato dimostro che le aziende meno preparate affrontano perdite medie di 5,10 milioni di dollari dopo una violazione dei dati mentre quelle ben addestrate riescono a limitare i danneggiamenti attorno ai 4,15 milioni di dollari. Questa evidenza sottolinea ulteriormente l'importanza di investire nella formazione del personale per ridurre i rischi e i costosi effetti delle violazioni informatiche.

Ulteriormente confermata da un'esplorazione condotta da Galinec, emerge il ruolo critico della limitata consapevolezza dei dipendenti come una delle principali vulnerabilità per la sicurezza

aziendale. Anche solo un dipendente non adeguatamente formato potrebbe compromettere l'integrità dell'intero piano di sicurezza informatica dell'azienda, mettendo così i dati e i sistemi aziendali ad un potenziale rischio elevato.

3.2 Il caso studio di Banca d'Italia: la percezione del rischio cibernetico delle imprese italiane

L'istituto Banca d'Italia[16] ha investigato sul tema della cybersecurity awareness per le imprese italiane, pubblicando gli articoli di Biancotti e Bencivelli nel 2016 e nel 2022. Lo studio ha approfondito il livello di *awareness*[17] delle imprese circa i rischi informatici e quanto queste siano in grado di adottare strategie in grado di limitare questi rischi. È emerso che circa il novanta per cento delle imprese ha la consapevolezza di incorrere in un attacco informatico, a questa però non sempre corrisponde un adeguata azione finanziaria per far fronte ai rischi. Le imprese che sono già state vittime di attacchi informatici, di qualsiasi gravità, mostrano una maggiore percezione e preparazione in materia, a cui si associa una più elevata propensione a fare investimenti. Questo perché, come abbiamo specificato le capitolo precedente, esiste una rilevante proporzionalità tra gravità del danno e costi di gestione e risposta. Dalle statistiche emerge che le imprese di minori dimensioni, e di conseguenza con minori fondi, risultano meno sensibili al tema e alle sue potenziali conseguenze [17]. Una possibile spiegazione è il fatto che, la maggior parte delle imprese italiane, e in particolar modo in Meridione, risultano piccole o medie imprese, le quali dispongono di più limitate risorse economiche per proteggersi, e in generale faticano ad inserirsi nella rivoluzione digitale. Comunque, in generale la consapevolezza delle potenziali conseguenze e dell'impatto cyber appare largamente diffusa tra le imprese, sebbene in misura diversa tra classi dimensionali e aree geografiche. Solo una minima parte delle aziende non ritiene ancora il rischio cyber potenzialmente dannoso, tra queste soprattutto le imprese piccole e residenti nel sud dell'Italia. Lo studio effaerma che il settore di appartenenza non sembra un fattore rilevante per spiegare differenze nei livelli di cybersecurity awareness: questo dato riflette l'analisi del secondo capitolo, in cui si può constatare che tutti i settori sono mediamente colpiti. I sondaggi successivi confermano che le determinanti ad incrementare gli investimenti in sicurezza informatica non sono ancora chiare, tuttavia, il fatto di aver subito già attacchi, ha determinato una maggiore propensione ad investire in infrastrutture e tecnologia di protezione [Figura 35].

[16] È la Banca centrale dello Stato Italiano e dell'economia italiana.
[17] Consapevolezza e preparazione.

	Quota imprese			Quota fatturato			
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
	No, perché non ha subito attacchi	No, ha subito attacchi ma senza danni	Sì	No, perché non ha subito attacchi	No, ha subito attacchi ma senza danni	Sì	Numero risposte
Area geografica							
Centro Nord	75,5	19,9	4,7	52,3	42,4	5,4	1.116
Sud e Isole	81,6	12,8	5,6	70,1	23,4	6,5	633
Numero di addetti							
20 - 49	80,5	15,2	4,3	77,3	18,9	3,8	562
50 e oltre	69,2	25,0	5,8	47,3	46,8	6,0	1.187
Totale industria in s.s e servizi	**76,6**	**18,5**	**4,8**	**54,0**	**40,5**	**5,5**	**1.749**

Figura 35: Danni patrimoniali da attacco cibernetico negli ultimi 5 anni (quota percentuale di imprese; pesati per rimando all'universo campionario e al totale del fatturato) [17]

Anche se il sondaggio afferma che la maggior parte delle aziende sia preparato in materia, questa tendenza non è confermata da azioni concrete, e da investimenti significativi. Questo fenomeno è spiegato dal fatto che i sistemi di prevenzione necessitino di aggiornamenti ciclici e di investimenti continui, che impattano sempre di più sul bilancio delle aziende. Circa un terzo delle aziende continua a non avere una funzione aziendale dedicata, [Figura 36] allo stesso tempo circa la metà ha dichiarato di aver aumentato gli investimenti negli ultimi cinque anni. Si può quindi pensare che tale aumento delle spese, non sia dovuto ad un effettivo investimento crescente in tecnologia di protezione, bensì alla semplice crescita dei costi delle tecnologie già presenti sul mercato. Dall'indagine emerge che la spesa per proteggersi contro la minaccia cyber risulta essere ancora molto limitata [Figura 37], in particolar modo le imprese maggiormente in difficoltà risultano le piccole imprese, organizzazioni meno al passo con la rivoluzione digitale e consapevoli del rischio informatico. Dunque, la dimensione dell'azienda risulta un fattore determinante sulla percezione del rischio informatico in Italia e sulla conseguente necessità di intraprendere investimenti in protezione e prevenzione.

		Sì			
	(1)	(2)	(3)	(4)	(5)
	No	Completamente interna	Ibrida	Completamente in outsourcing	Numero risposte
Area geografica					
Centro Nord	4,7	52,3	42,4	5,4	1.116
Sud e Isole	5,6	70,1	23,4	6,5	633
Numero di addetti					
20 - 49	4,3	77,3	18,9	3,8	562
50 e oltre	5,8	47,3	46,8	6,0	1.187
Totale industria in s.s e servizi	**4,8**	**54,0**	**40,5**	**5,5**	**1.749**

Figura 36:Funzione aziendale dedicata alla cybersicurezza e alla continuità operativa [17]

	(1) Non è sostanzialmente cresciuta	(2) È cresciuta, ma meno che raddoppiata	(3) È più che raddoppiata	(4) Numero risposte
Area geografica				
Centro Nord	45,6	41,1	13,3	1.100
Sud e Isole	67,4	25,7	6,9	625
Numero di addetti				
20 – 49	56,4	33,2	10,4	559
50 e oltre	36,6	48,1	15,4	1.166
Totale industria in s.s e servizi	**49,7**	**38,2**	**12,1**	**1.725**

Figura 37: Variazione spesa sostenuta contro attacchi cibernetici negli ultimi 5 anni (%imprese) [17]

L'Agenzia dell'Unione Europea per la cybersecurity ha evidenziato di come non sia sufficiente rispettare le normative e le politiche aziendali, ma sia fondamentale una maggiore consapevolezza dei rischi associati alla sfera digitale da parte di tutto il personale. Questo coinvolgimento attivo comporta una maggiore efficacia nel rendere marginale il rischio cyber.

3.3 Programmi di formazione efficaci sulla sicurezza informatica

La formazione del personale è da ritenersi fondamentale per accrescere la Cybersecurity Awareness. Sensibilizzare i dipendenti ad avere una forte motivazione di tutela dell'azienda agevola maggiormente la capacità di affrontare e superare le minacce informatiche. Purtroppo spesso non viene percepito come parte specifica ed essenziale della responsabilità di ciascuno, ma la capacità di essere formati e preparati a queste evenienze è da considerarsi parte integrante del lavoro di ciascun dipendente. Presupposto e conseguenza della scarsa formazione sono la presenza di programmi di approfondimento sulla sicurezza poco efficaci. In altri casi invece è stato riscontrato che nonostante vengano seguite tutte le procedure di sicurezza, tuttavia la formazione continua a non essere un fattore chiave per prevenire il rischio cyber. Questo si verifica soprattutto quando la modalità di erogazione della formazione avviene in poche ore e con modalità obsolete, di conseguenza, viene percepita come uno spreco di tempo da tutti i partecipanti che tenderanno probabilmente ad agire come prima. Stesso risultato lo si avrà nel momento in cui le informazioni vengono trasmesse in modo confusionario ed eccessivo.

Un programma di Cybersecurity Awareness efficace deve includere:

- Una corretta definizione del livello di competenza e degli obbiettivi:
  - Gli obbiettivi devono essere standard almeno del settore di appartenenza dell'azienda;
  - Una corretta taratura tra il livello di preparazione desiderato e il tempo di formazione;
- Bisogna rendere preparati tutti i dipendenti almeno per tutte le attività quotidiane di lavoro e quindi per i rischi che quotidianamente potrebbero incontrare:

    - Tramite moderne tecniche di apprendimento, ad esempio tramite tools specifici e automatici;
    - Ripetere i test e le valutazioni ciclicamente, per mantenere i livello di preparazione necessario;
- Controllare e aggiornare continuamente la formazione, perché le minacce informatiche si evolvono continuamente:
    - Definire obbiettivi annuali di formazione e monitorarli continuamente;
    - L'idea è quella di prevenire il più possibile, invece che rispondere. Il monitoraggio delle aree maggiormente a rischio e le relative decisioni da intraprendere;
    - Analizzare l'andamento dei corsi e comparare i reparti e la loro preparazione;
- L'attuazione dei corsi deve essere consona con la formazione richiesta:
    - Moderne tecniche di apprendimento per stimolare l'attenzione;
    - Fare continui esempi di attività quotidiane azzardate;
    - Favorire la comunicazione e la cultura aziendale;

L'azienda di soluzioni di prodotti informatici Kaspersky ha proposto un nuovo programma di formazione sulla cybersecurity, differenziato per le diverse tipologie di dipendenti e i diversi livelli gerarchici delle organizzazioni. È un approccio che sta avendo notevole successo e sta producendo risultati significativamente positivi. L'azienda segue in linea di principio le linee guida spiegate precedentemente, poiché basa la formazione su moderne tecniche di apprendimento, immersive e stimolanti, finalizzate a costruire questa cultura della prevenzione alle minacce informatiche. L'approccio è basato su piattaforme interattive, giochi di squadra, monitoraggio dei risultati ed esempi continui basati su episodi quotidiani.

La formazione sulla cybersecurity include:

1. Come individuare e segnalare attacchi di phishing;
2. Come usare in modo sicuro supporti rimovibili;
3. Come creare password complesse e come implementare l'autenticazione a più fattori;
4. Come garantire la protezione di dispositivi fisici e documenti;
5. Come usare i dispositivi mobili in tutta sicurezza cd. sicurezza mobile;
6. Individuare il modo di stare al sicuro lavorando in smart working, inclusi i rischi dell'utilizzo di un Wi-Fi pubblico;
7. Come orientare il personale nell'uso sicuro di applicazioni basate su cloud;

8. Individuare le tecniche più comuni utilizzate dai criminali informatici e l'influenza della psicologia, quella che prende il nome di social engineering;
9. Come monitorare e gestire i dati aziendali in modo sicuro;
10. Come installare programmi software e applicazioni di terze parti in tutta sicurezza nei computer aziendali;
11. Informare su procedure di risposta agli avvisi per affrontare e gestire i rischi per i sistemi informatici;
12. Comprendere l'ambiente normativo per lo specifico settore e quello che implica in termini di cybersecurity.

L'approccio innovativo di Kaspersky Lab si basa su moderne tecniche di apprendimento che contribuiscono alla costruzione di interessanti dinamiche sociali di gruppo: è una metodologia che combina metodi di assimilazione di conoscenze attraverso attività pratiche e rafforzamenti dei concetti. Tra questi, l'approccio alla formazione tramite piattaforme interattive rappresenta la chiave per formare il comportamento delle persone e per costruire nuove dinamiche comportamentali rendere le persone consapevoli dei pericoli rappresentatitramite il confronto e le discussioni durante le attività di gruppo [Figura 38].

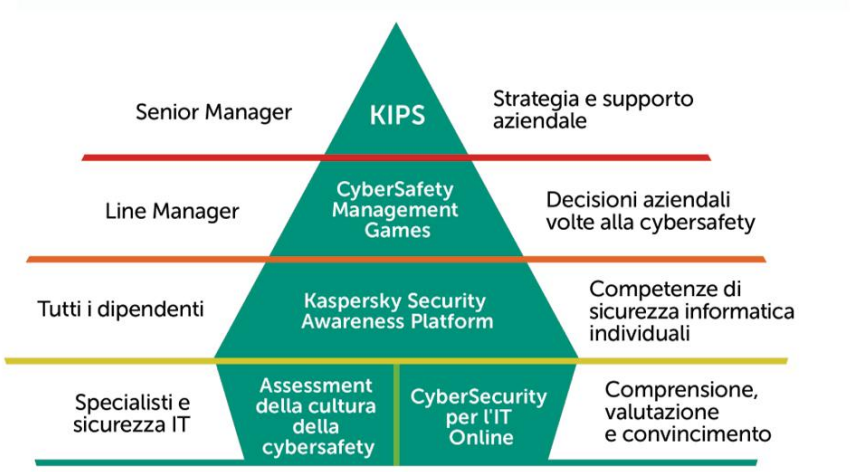

Figura 38: Programmi di formazione Kaspersky Lab [15]

Kaspersky Interactive Protection Simulation (KIPS):

Il KIPS è il primo programma proposto dall'azienda. Esso si basa su una piattaforma ludica, in cui diverse squadre si scontrano e si mettono a confronto su determinati scenari incontrati. Il suo obbiettivo è quello di preparare il personale dei reparti IT e i manager a delle situazioni di attacco

simulate, e a prendere le giuste decisioni, cercando di salvaguardare l'efficienza dei costi, la continuità del business, l'architettura hardware e software e l'immensa mole di dati gestita dall'azienda. Questo approccio innovativo permette di comprendere come determinati attacchi informatici possano causare ingenti costi, disordine e ridurre la redditività. La piattaforma offre simulazioni per qualsiasi settore esistente, in modo da formare le persone in modo più completo possibile sulle criticità più comuni dei loro settori. Questo approccio contribuisce a costruire un'unità di intenti e di pensiero sul tema della cybersecurity, perché la simulazione dell'attacco permette di prendere decisioni di risposta e permette di vedere le conseguenze manifestate. Una corretta comunicazione e un piano strategico di risposta sono la base per poter limitare i danni patrimoniali degli attacchi informatici. Le decisioni da prendere, ad esempio, possono intaccare la produzione, la perdita di clienti, la perdita di ricavi e inoltre possono simulare se il budget in cybersecurity stanziato sia stato sufficiente a coprire questi spiacevoli episodi. L'idea è quella che con una simulazione di un attacco e con la conseguente gestione post-attacco, si possa costruire molto più efficacemente una cultura della cybersecurity forte e resiliente. Non è più sufficiente solamente seguire semplici corsi di formazione in sedute di poche ore, perché questo approccio non ha portato i risultati sperati. Grazie a queste moderne tecniche di apprendimento, il management potrà agire in maniera più consapevole e potrà estendere ciò che ha appreso a tutta l'organizzazione.

Kaspersky Cybersafety Management Games:

I "Kaspersky Cybersafety Management Games" forniscono ai middle manager le competenze, le conoscenze e gli atteggiamenti essenziali e corretti per mantenere sicuro il proprio ambiente di lavoro IT relativo alla loro divisione. È un programma che cerca di coprire tutte le principali situazioni e ambiti tipiche delle business unit, tramite brevi moduli, esempi, spiegazioni ed esercizi. I manager sono quindi addestrati ad individuare una minaccia e cercare di mitigarla, intraprendendo le giuste azioni. I risultati di questa formazione devono essere [Figura 39]:

- Comprensione delle azioni quotidiane importanti ma non eccessivamente complicate per garantire sicurezza informatica.
- Considerare la sicurezza informatica come parte integrante dei processi aziendali.
- Acquisire una leadership nei confronti dei dipendenti in tali ambiti.

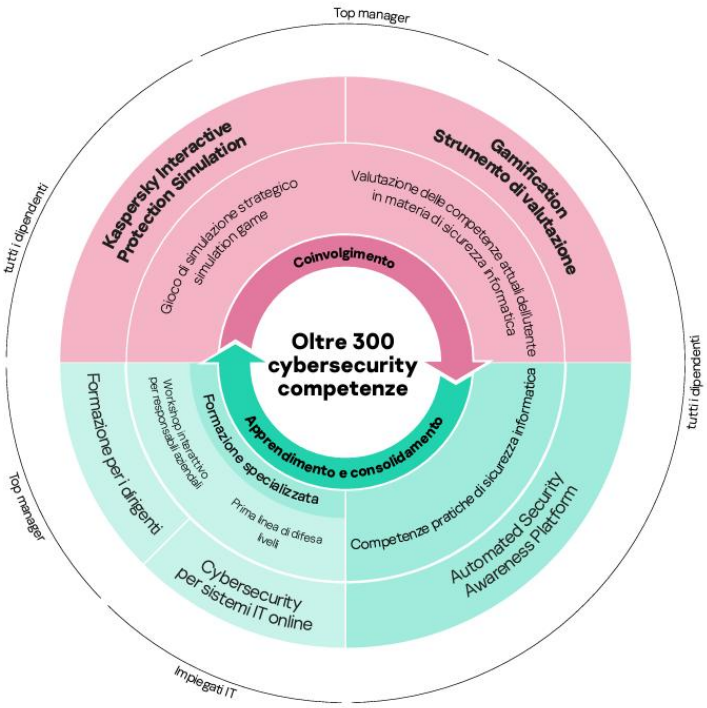

Figura 39: L'intero programma offerto da Kaspersky [15]

Kaspersky security awareness platform:

Una piattaforma di apprendimento online che sviluppa *l'awareness* sulla sicurezza informatica finalizzate a dare competenze pratiche, salvaguardando la sicurezza della rete e offrendo ai dipendenti la conoscenza necessaria per lavorare senza limiti. Vengono proposti corsi di formazione, per aziende di qualsiasi dimensione, con lezioni pratiche e interattive, test e simulazioni di attacchi.

Questo approccio ha già registrato i seguenti risultati [15]:

- Calo numerico di incidenti fino al 90%
- Riduzione dell'impatto finanziario degli incidenti di almeno il 50%
- L'86% di chi ha partecipato a questi corsi di formazione lo ha ritenuto utile e consigliabile
- 93% è la probabilità di utilizzare queste conoscenze nel lavoro quotidiano
- Ritorno degli investimenti sui prodotti di cybersecurity awareness superiore al 30%

In conclusione di questo capitolo, si può affermare che risulti fondamentale rendere le persone consapevoli dei rischi informatici e delle conseguenze che si possono generare. Per fare ciò risulta necessario rinnovare il modo di pensare del passato, secondo cui l'errore umano era considerato l'anello debole della sicurezza informatica, e pensare che tutte le persone possano essere la prima

linea di difesa e prevenzione, e non solo il personale addetto alla sicurezza informatica. Questa transizione sicuramente sarà accompagnata dall'educazione, che dovrà essere sempre più efficace e dovrà contribuire a porre la cybersecurity al centro delle strategie aziendale e al centro della continuità del business.

4. Il ruolo delle policy a sostegno dell'educazione digitale

Parallelamente allo sviluppo di internet è sorta la necessità di formulare una normativa idonea e organica in materia di cybersecurity. Da subito si sono potute intuire le conseguenze dannose degli attacchi informatici, i quali possono determinare significativi danni alle libertà sancite dalla nostra carta costituzionale. Dunque la sicurezza informatica diventa fondamentale non solo per il corretto funzionamento delle attività di organizzazioni e stati, ma anche per tutelare diritti fondamentali legati alle attività digitali, tra cui spicca la confidenzialità dei dati [18].

La sempre più crescente complessità nel gestire le minacce informatiche e la loro natura sempre più in costante evoluzione, necessita l'adozione di un coordinamento internazionale e di norme il più possibile condivise tra stati. Infatti l'Unione Europea ha definito un ampio ventaglio di normative, direttive e regolamenti volti a definire tale ambito, al fine di proteggere i singoli individui nelle loro attività online, le aziende e le istituzioni [19]. Anche l'Italia, come gli altri paesi UE, sta cercando di applicare la normativa sovranazionale.

In questo capitolo verrà analizzato prima il quadro normativo europeo, e successivamente la situazione normativa italiana. Accanto a queste normative, per completezza, verrà esposta la norma internazionale di tale materia, definita dall'International Organization For Standardization.

4.1 L'ordinamento UE

I fondamenti normativi in materia di cybersecurity sono stati definiti dall'Unione Europea. Risalgono agli anni novanta le prime norme volte ad inquadrare l'ambiente digitale, tuttavia solo nel 2004 fu messo in atto il primo "vero" grande intervento, che ha portato alla nascita dell' **l'European Union Agency for Cybersecurity,** ossia l'**ENISA**[18]. Si tratta di un'agenzia istituita al fine di concentrare in capo ad un unico soggetto la gestione della politica informatica europea e di progettare il piano strategico di sicurezza informatica comune agli Stati membri. Con il passare degli anni questa agenzia ha assunto un ruolo sempre più importante accompagnato da un'espansione delle sue competenze, anche perché, come abbiamo detto più volte, tale materia è sempre più complessa e impattante su tutti gli individui[19].

[18] Regolamento (CE) n. 460/2004 adottato dal Parlamento europeo e dal Consiglio. Istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione, attribuendole il compito di assicurare un elevato livello di sicurezza delle reti nonché a promuovere una cultura in materia a favore della popolazione, dei consumatori, delle società e delle organizzazioni del settore pubblico nell'Unione europea.

[19] Il ruolo dell'ENISA è stato rafforzato precedentemente con il Regolamento n. 526/2013, in seguito con il Cybersecurity Act nel 2019.

Un passo fondamentale è stato fatto con l'emanazione della **Direttiva NIS**, acronimo di Network And Information Security[20], adottata nel 2016 ad opera del Parlamento Europeo e del Consiglio e attuata in Italia due anni dopo. Questa delinea, per la prima volta nella storia, parametri di sicurezza informatica comuni e uniformi tra gli Stati membri [21]. Con la direttiva NIS si perseguono diversi obbiettivi, tra cui il miglioramento delle infrastrutture, l'adozione di misure preventive robuste e di gestione del rischio cyber. Con questa direttiva, l'Unione Europea non ha solo dettato delle norme astratte, ma, al fine di garantire un pari livello di sicurezza, ha definito target minimi da rispettare. In particolare ha individuato i destinatari di questa disciplina: gli "operatori economici di servizi essenziali" e i "fornitori di servizi digitali". Ciascuno, all'interno della propria categoria, deve sottostare agli obblighi finalizzati ad adottare strumenti tecnici e organizzativi di prevenzione in cybersecurity.

Sempre più necessaria l'esigenza di aumentare i livelli di sicurezza delle infrastrutture e di tracciare un quadro organico finalizzato a coordinare la disciplina della cybersecurity, ha portato il Parlamento europeo ad emanare il **Cybersecurity Act** [21]. Attraverso lo strumento del regolamento, che assicura la diretta applicabilità delle disposizioni, l'unione ha posto l'obbiettivo di creare un mercato unico digitale più protetto attraverso l'inserimento di un meccanismo di certificazione europea. Inoltre, il Cyber Act ha rafforzato il ruolo dell'ENISA, attribuendole la funzione indispensabile di coordinamento finalizzata a garantire un coeso livello di sicurezza informatica all'interno dei paesi aderenti all'Unione Europea.

L'affermazione di principi e di norme comuni in materia di cybersecurity, allo scopo di porre fine alle crisi dovute ai diversi livelli nazionali di risposta a fronte di attacchi cyber, è molto importante ricordare la **Direttiva NIS 2**[22] e la proposta di Regolamento **Cyber Resilience Act** [22]. La direttiva NIS 2 [23], proposta dalla Commissione alla fine del 2020, è entrata in vigore nel gennaio 2023, sostituisce la disciplina previgente del 2016, ritenuta inefficace a rispondere alle più moderne tecniche di attacco.

Questa nuova normativa opera un allargamento dell'ambito di applicazione dei vincoli e degli standard di sicurezza informatica, comprendente una più ampia cerchia di soggetti con la finalità

[20] Direttiva UE 2016/1148 del Parlamento europeo e del Consiglio, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
[21] Regolamento UE 2019/881 del Parlamento europeo e del Consiglio, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il Regolamento (UE) n. 526/2013. Consultabile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32019R0881.
[22] Direttiva UE 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del Regolamento UE n. 910/2014 e della Direttiva (UE) 2018/1972 e che abroga la Direttiva (UE) 2016/1148.

di dare una copertura integra dei settori ritenuti più importanti. Questa direttiva assegna, mediante regole chiare e precise che non lasciano spazio all'incertezza, precisi doveri di gestione e pone in luce importanti indicazioni sui rischi in materia di cybersicurezza (precisamente artt. da 17 a 23) e sancisce obblighi in materia di condivisione delle informazioni (artt. 26 e 27) a tutti gli operatori del settore. È possibile dividere i soggetti destinatari di tali obblighi tra "soggetti essenziali" e "soggetti importanti": rispettivamente i primi sono coloro che operano nei settori quali energia, trasporti, bancario e sanitario, mentre i secondi sono coloro che operano nei settori dei servizi postali, gestione rifiuti, fabbricazione, produzione e distribuzione. La ratio di questa divisione risiede nel proposito di evitare di sottoporre ugualmente tutti gli operatori all'interno di un unico quadro di obblighi e doveri, si indica invece un regime differenziato, a seconda dell'attività svolta, che tenga conto del rischio di alcuni settori rispetto ad altri, che potrebbero subire conseguenze più gravi in caso di violazioni. In questo ambito la Direttiva NIS 2 è rilevante anche perché i soggetti operanti potranno beneficiare del vantaggio di poter individuare gli ambiti prioritari su cui intervenire per colmare le carenze e ridurre le debolezze informatiche a cui rimarrebbero altrimenti esposti. Questo meccanismo li indurrà ad adottare misure tecniche proporzionate e adeguate, nonché ad assumere una maggiore responsabilità in considerazione del regime di vigilanza a cui sono assoggettati e delle correlate misure sanzionatorie.

Un altro atto giuridico importante adottato dalla Commissione europea nel 2022 è il **Cyber Resilience Act** [23], con questo regolamento il legislatore ha delineato un quadro dettagliato di impegni e requisiti uniformi di cybersicurezza, ai quali i soggetti destinatari degli Stati membri, sono tenuti a adeguarsi a seconda dei prodotti con elementi digitali che intendono introdurre nel mercato interno. Questo atto è finalizzato alla salvaguardia di consumatori e imprese anche da prodotti digitali caratterizzati da livelli di sicurezza non adeguati.

Questa approccio distintivo di obblighi e requisiti della categoria di appartenenza dei soggetti e della specialità dei prodotti è finalizzato a creare le condizioni per lo sviluppo di prodotti con elementi digitali sicuri già dalle origini del ciclo di vita del prodotto. Questo principio prende il nome di "security by design" richiede ai soggetti operanti nel settore di agire in modo preventivo eliminando, sin dalle prima fasi di progettazione e produzione dei prodotti con elementi digitali, le vulnerabilità e i pericoli connessi ad essi.

[23] Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali. Consultabile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454.

Questo approccio si basa sul principio di proporzionalità delle misure tecniche, in quanto gli operatori del settore saranno tenuti a attivare, in base al livello di rischio associato ai loro prodotti, già precedentemente individuato dalla normativa, misure tecniche proporzionate e adatte alla loro esigenza. Tutto questo, indirettamente, determina un ampliamento della responsabilizzazione degli operatori, i quali, nel conformarsi ai requisiti stabiliti dal legislatore, assumeranno la responsabilità del proprio operato attraverso un comportamento proattivo idoneo all'applicazione del regolamento.

Per concludere con l'analisi delle fonti europee, si deve trattare un ulteriore regolamento cd. **Digital Operational Resilience Act**[24] adottato nel dicembre 2022, definisce una struttura comune di risposta operativa digitale per tutti gli operatori del settore finanziario vincolandoli a rispettare una serie di requisiti di sicurezza informatica. Questa disciplina è stata pensata perché anche i sistemi informatici aziendali si trovano in una crescente, e sempre più continua, condizione di vulnerabilità nei confronti di possibili attacchi informatici.

Sulla base di tali fondamenta, si è sviluppata successivamente la legislazione nazionale in materia di cybersicurezza che vedremo.

4.2 L'ordinamento italiano

L'Italia, seguendo le regole imposte dall'Unione Europea, si è impegnata nell'attuazione di norme volte a definire tale disciplina. Tuttavia, a differenza di altri stati membri, si è sempre distinta per i notevoli ritardi nell'attuazione di risposte, il che la rende in molte statistiche uno degli stati più povero e indietro in tale contesto.

Il primo macro-evento è avvenuto il 24 Gennaio 2013, con l'emanazione del **DPCM**[25] ad opera di **Monti**[26]. Questo decreto ha messo in atto le prime linee guida in materia e ha fatto nascere nuovi organi istituzioni, come il Nucleo per la Sicurezza Cibernetica. Inoltre si è concentrato sul definire i modi di interagire tra esso e tutte le altre istituzioni, fino ad arrivare al Presidente del Consiglio dei Ministri.

[24] Regolamento UE 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario. Consultabile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554.
[25] Decreto del presidente del consiglio dei ministri
[26] Decreto del Presidente del Consiglio dei ministri, 24 gennaio 2013, Direttiva sugli indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, attraverso il quale è stata delineata una prima architettura della materia fondata su due distinti documenti: il "Quadro nazionale per la sicurezza dello spazio digitale" e il "Piano nazionale per la protezione cibernetica e la sicurezza informatica". Consultabile al seguente indirizzo: https://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg.

Un successivo passo viene fatto nel 2017, con il nascere di un altro **DPCM**, ad opera del primo ministro **Gentiloni**. Questo ha aggiornato le strategie da seguire iniziate nel 2013 con il nuovo panorama della cybersicurezza, e ne ha esteso le aree di competenza, fino ad arrivare alla costruzione di un vero e proprio Piano Nazionale[27].

Tuttavia, il primo vero intervento in materia di cybersecurity è arrivato in Italia nel 2018 con il **decreto legislativo NIS** o **decreto legislativo 65/2018**, in conseguenza della direttiva europea Network and Information Security. Con questo nasce il Perimetro di sicurezza nazionale cibernetica, il quale ha irrobustito notevolmente il quadro normativo nazionale, che allora risultava molto indietro rispetto ad altri stati. Il Perimetro di sicurezza nazionale cibernetica [24] è stato strutturato al fine di garantire un elevato livello di sicurezza per le reti, per i servizi in rete e per le amministrazioni pubbliche e private.

Un altro passo importante è stato fatto col decreto-legge 14 giugno 2021, il quale sancì l'istituzione di tre organi fondamentali per la sicurezza informatica, ossia l'**Agenzia per la cybersicurezza nazionale**, il **Comitato interministeriale per la cybersicurezza** e il **Nucleo per la cybersicurezza**. La prima è l'organo con l'obbiettivo garantire la cybersecurity sul territorio nazionale, e di costruire la strategia di nazionale per la sicurezza informatica. Il secondo è l'autorità con il compito di monitorare questa strategia, e di supportare le politiche in materia di cybersecurity e il Perimetro della sicurezza nazionale. Il terzo organo invece è stato istituito per assistere ed aiutare il Presidente del Consiglio dei ministri nell'attuazione di norme volte alla prevenzione di attacchi cibernetici. L'operato di questi tre organi, tuttavia, è stato reso effettivo solamente il 17 maggio 2022, con l'effettivo inserimento di fondi dedicati nella legge di bilancio. Questo è un ulteriore episodio che mostra l'incapacità del nostro paese di adottare con tempestiva efficacia strategie di prevenzione in materia di cybersecurity, e non solo [25].

Il **Piano Nazionale di Ripresa e Resilienza o PNRR** ha dedicato diverse sezioni alla cybersecurity, al fine di garantire un infrastruttura digitale sicura contro le minacce informatiche sempre più difficili da intercettare. Quasi il 20 percento delle risorse totali investite è destinato a tale ambito. Questa percentuale riflette il fatto che la cybersecurity sia la prima delle sei missioni delineate dal PNRR, e infatti sono destinate massicce risorse economiche. Più dettagliatamente il Piano destina un importo di quasi 40 Miliardi di euro. Di questi, circa il due percento è interamente rivolto alla

[27] È stata comunicata sulla Gazzetta ufficiale n. 125 del 31 maggio 2017 l'adozione del nuovo Piano nazionale per la protezione digitale e la sicurezza informatica: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf.

"digitalizzazione, innovazione e sicurezza nella PA[28]", questi finanziamenti sono destinati a tre aree:

- Miglioramento delle capacità di prevenzione dagli attacchi cibernetici;
- Miglioramento di infrastrutture informatiche più sicure e che riescano a garantire l'erogazione continuative dei servizi;
- Aumento del personale addetto alla cybersecurity;

Da questa analisi dell'ordinamento italiano emerge un attenzione crescente in materia di cybersicurezza, in linea con le disposizioni europee e con le tendenze comunitarie. Tuttavia, la Corte dei conti europea ha individuato continui ritardi nell'implementazione delle norme di cybersicurezza previste dalla NIS 2. Nonostante i 67,5 milioni di euro dal PNRR investiti, l'Italia si è ridotta solamente ad attuare analisi preliminari di rischio, senza intraprendere azioni complete di prevenzione e procedure di sicurezza concrete. Infatti, dei dieci obbiettivi individuati dalla normativa NIS 2, l'Italia ha limitato l'azione alla fase analitica. Le iniziative previste appaiono ambiziose, ma la loro implementazione concreta è ancora troppo lenta e disorganizzata per rispondere efficacemente alle minacce. Questo ritardo non solo riduce la capacità competitiva del Paese sul piano internazionale, ma espone maggiormente l'Italia a minacce cibernetiche, infatti, come ha rilevato la Corte, gli attacchi informatici nel 2023 sono aumentati al 169%, questo comporta gravi conseguenze economiche e di sicurezza.

Nonostante gli sforzi e i progetti portati avanti dalla Polizia Postale e dal Security Operation Center, l'Italia rimane indietro rispetto ad alcuni paesi europei. Purtroppo questo esito negativo nell'attuazione delle misure del PNRR riflette una inclinazione della Pubblica Amministrazione italiana alla inefficace gestione dei fondi comunitari.

Le criticità italiane più importanti risultano:

1. **Ritardi nell'implementazione delle normative**: L'Italia ha spesso mostrato lentezza nell'adeguamento alle direttive europee, come dimostrato dal tardivo recepimento della Direttiva NIS e dalle difficoltà nella preparazione per la NIS 2.
2. **Mancanza di coordinamento**: A differenza di altri Paesi europei con agenzie centralizzate dedicate alla cybersecurity, in Italia la gestione è frammentata tra diverse istituzioni (AGID, ACN, Ministero della Difesa, ecc.), il che complica l'attuazione di politiche efficaci.

[28] Pubblica Amministrazione

3. **Carenza di risorse**: Le risorse finanziarie e umane destinate alla cybersecurity sono limitate rispetto ad altri Paesi europei. Ad esempio, l'Italia investe meno nel settore rispetto a Germania e Francia, sia in termini di spesa pubblica che privata.

4. **Formazione e consapevolezza**: La cultura della cybersecurity è meno sviluppata in Italia. Molte aziende, in particolare le PMI, non sono sufficientemente preparate a fronteggiare attacchi informatici, anche a causa di una limitata consapevolezza e formazione specifica.

5. **Certificazione e standard**: L'Italia non ha ancora sviluppato un sistema di certificazione della sicurezza informatica in linea con il Cybersecurity Act, il che limita la competitività delle imprese italiane nel mercato europeo.

Per colmare il divario con l'Europa, l'Italia deve affrontare alcune sfide chiave: accelerare l'implementazione delle normative, migliorare il coordinamento istituzionale, investire in risorse e formazione, e sviluppare un sistema di certificazione efficace. Solo attraverso un approccio integrato e strategico sarà possibile garantire un livello di cybersecurity allineato agli standard europei e adeguato alle sfide attuali. Ormai appurata la complessità del tema e della relativa attuazione di normative, è sempre più importante che le regolamentazioni siano efficaci e flessibili, sia per il legislatore europeo, sia per quello italiano. Solo facendo così si può cercare di arginare questi rapidi cambianti in materia. Un ulteriore aspetto importante è cercare di uniformare il più possibile queste normative e rendere più condivise possibili queste regole, al fine di limitare le disparità sui livelli di sicurezza, almeno per tutti gli stati membri dell'Unione Europea. Solo facendo così si può effettivamente costruire una strategia di gestione della cybersecurity resiliente e condivisa.

4.3 La norma internazionale ISO/IEC 27000

Per completare questa panoramica sul quadro normativo internazionale, risulta necessario introdurre e descrivere i contenuti della norma internazionale che tratta questa materia. La norma internazionale è la ISO/IEC 27000, dove per l'acronimo ISO si intende l'ente internazionale International Organization for Standardization[29], invece per IEC si intende International Electrotechnical Commission[30]. Lo standard ISO/IEC 27000 fa parte degli standard internazionali, contenente il tema della sicurezza dell'informazione e della sua gestione normativa. Come è stato

[29] International Organization for Standardization: è un'organizzazione indipendente, non governativa, i cui membri sono le organizzazioni di normazione dei 162 paesi membri.
[30] International Electrotechnical Commission: è un'organizzazione internazionale non profit, non governativa che prepara e pubblica norme internazionali relative al settore dell'elettrotecnica.

spiegato nel primo capitolo, questo tema emerge a partire dagli anni ’90, tanto che lo standard internazionale viene pubblicato nel 1992, fino ad arrivare alla sua ultima revisione nel 2024. La famiglia delle ISO/IEC 27000 comprende:

- ISO/IEC 27001: È uno standard internazionale per i sistemi di gestione della sicurezza delle informazioni (ISMS). Definisce i requisiti per implementare, mantenere e migliorare continuamente un sistema di gestione della sicurezza.
- ISO/IEC 27002 : Fornisce una serie di controlli di sicurezza e linee guida per implementare le misure richieste da ISO/IEC 27001.
- ISO/IEC 27003: Linee guida per l’implementazione dell’ISMS
- ISO/IEC 27004: Misure di gestione della sicurezza delle informazioni
- ISO/IEC 27005: Specifica i metodi per la gestione dei rischi legati alla sicurezza delle informazioni.
- ISO/IEC 27006: Requisiti per l'accreditamento degli organismi che forniscono la certificazione ISMS.
- ISO/IEC 27007: Linee guida per l'audit ISMS.

Si affiancano a queste norme anche altre disposizioni internazionali che definiscono le linee guida da seguire per l’implementazione di un sistema di gestione per la sicurezza delle informazioni attraverso un processo specifico e standard minimi per qualsiasi settore.
Strutturalmente la ISO/IEC 27000 è costituita da quattro capitoli:

1. Ambito
2. Termini e definizioni
3. Information security management systems
4. ISMS standard di famiglie

Lo scopo di queste normative è quello di costruire una panoramica generale sulla gestione della sicurezza delle informazioni. L’information security management system viene definito come un insieme di politiche, procedure, linee guida, risorse ed attività, gestite da un’organizzazione al fine di proteggere i propri dati e asset informativi. È un approccio generale per stabilire, attuare, monitorare e migliorare la sicurezza delle informazioni di un’azienda, per renderle conformi alle normative. Al fine di ottenere questo risultato, l’ISMS si incentra su un’attenta valutazione e sulla successiva mitigazione del rischio, entro il livello stabilito dalla direttiva aziendale. La norma definisce i principi che contribuiscono alla corretta adozione dell’ISMS:

1. Consapevolezza dell’organizzazione sulla centralità della sicurezza delle informazioni;
2. Attribuzione di responsabilità a individui diversi dell’organizzazione in tale ambito;

3. Ruolo centrale dell'alto management e degli stakeholders aziendali sulla sua corretta attuazione;
4. L'ISMS aiuta il rafforzamento dei valori aziendali;
5. Valutazione dei rischi tramite un processo strutturato di monitoraggio, al fine di rientrare all'interno della soglia di accettazione stabilita dalla governance dell'organizzazione;
6. Inquadrare la sicurezza come elemento chiave delle reti e dei sistemi informativi aziendali;
7. Adottare un sistema di prevenzione attiva e di rilevazione di incidenti;
8. Garantire un approccio completo e strutturato alla gestione della sicurezza delle informazioni;
9. Ciclica rivalutazione dell'attuale sistema di sicurezza delle informazioni, applicando le opportune modifiche migliorative;

Come si è potuto evincere, le minacce alla sicurezza informativa provengono da moltissime fonti, è dunque importante per qualsiasi organizzazione adottare un sistema di sicurezza delle informazioni, perché grazie ad esso sarà in grado di affrontare i rischi connessi alle risorse informative. La ISO/IEC 27000 sancisce la centralità dell'adozione di un ISMS, sia per il settore privato che pubblico, in quanto è fondamentale per garantire la sicurezza informativa mediante processi e procedure ben definite in grado di limitare i rischi connessi ad una perdita o danneggiamento dell'informazione stessa. In questo modo si ottiene un organizzazione in grado di avere una maggiore protezione delle risorse informative contro le minacce, ottenere un quadro strutturato e globale per identificare e valutare i rischi che incombono sulla sicurezza delle informazioni, così da adottare gli adeguati controlli e migliorarne la loro efficacia. Ancora è importante al fine di migliorare continuamente l'ambiente di controllo e realizzare in modo efficace la conformità legale e normativa.

Per permettere all'organizzazione di soddisfare i propri target, vengono di seguito affermati gli otto fattori chiave di successo di un ISM:

1. Allineare gli obiettivi della policy sulla sicurezza delle informazioni con le attività e gli obiettivi strategici aziendali;
2. Un framework per la progettazione, l'attuazione, il controllo costante, il mantenimento e il miglioramento dell'ISMS in linea con i principi aziendali;
3. Impegno da parte di tutti i componenti dell'organizzazione a qualsiasi livello, ma in particolar modo dall'alto management;
4. Comprensione dei requisiti di protezione dei dati attraverso l'applicazione dell'ISMS ISO/IEC 27005

5. Un’attenta sensibilizzazione alla sicurezza delle informazioni per i dipendenti, i quali devono essere informati dei loro obblighi, contenuti nella policy della sicurezza delle informazioni e nelle norme, motivandoli a rispettare questi impegni;
6. Un’efficace processo di gestione degli incidenti informatici rilevati;
7. Un approccio mirato alla continuità operativa aziendale;
8. L’utilizzo di un corretto sistema di misurazione e rilevazione, per la valutazione delle prestazioni ottenute grazie all’implementazione dell’ISMS.

Un’efficace implementazione di un ISMS, rispettando i fattori chiave di successo sopra enunciati, permetterà all’organizzazione di raggiungere i propri obiettivi proteggendo i propri asset informativi.

Conclusioni

La domanda di partenza di questo elaborato era capire perché e come la cybersecurity impatti sulla continuità aziendale e sull'economia. I principali fattori che hanno contribuito a mettere in luce la cybersecurity come disciplina fondamentale sono l'incremento dell'utilizzo degli strumenti informatici in molteplici attività e la conseguente crescita degli attacchi informatici.

Al fine di risolvere questo problema, o almeno cercare di arginarlo, è stata affermata la necessità di avere un'organica regolamentazione di questa materia e l'esigenza di formare soggetti in grado di gestire queste sfide. Tutto questo è imprescindibile se si pensa alla tecnologia, che, a causa dei suoi naturali cambiamenti, richiede una regolazione flessibile e adattabile ad ogni esigenza. In secondo luogo, occorre precisare che non basta la predisposizione di norme in risposta ai continui progressi tecnologici, ma occorre agire anche sui soggetti, in quanto sono le azioni umane che spesso compromettono la sicurezza informatica. Non vi sarà mai un sistema tecnico così perfetto o una regolazione talmente efficace da poter sostituire la responsabilità umana nell'uso della tecnologia.

Sempre di più ci si sta accorgendo della necessità di adottare precauzioni in materia di cybersecurity: la loro mancata adozione può essere imputata alla combinazione di motivi diversi, fra i quali emerge sicuramente una carente educazione digitale, ossia l'assenza di adeguate competenze digitali minime in capo alla generalità dei soggetti. Infatti, per ridurre l'impatto del fattore umano sui rischi cyber è indispensabile investire nella formazione degli individui. È necessario sottolineare e riconoscere che il dominio della sicurezza informatica non può essere esclusivamente ancorato all'ambito tecnico e ai vincoli normativi, ma richiede altresì un'indispensabile assunzione di consapevolezza proattiva in merito ai rischi connessi all'uso degli strumenti informatici. E' importante che questa consapevolezza non si limiti alla mera adozione di pratiche basilari di precauzione digitale e buone abitudini di sicurezza, ma è fondamentale che si estenda anche all'allocazione di risorse, economiche e non, verso programmi e iniziative finalizzate a promuovere una maggiore responsabilizzazione verso la cyber sicurezza e a fornire ai dipendenti aziendali, ma anche a soggetti comuni, una formazione adeguata su come affrontare i pericoli della rete. Proprio in questo aspetto, i dati attuali non sono affatto positivi: secondo l'indice DESI[31] del 2024, basato sui dati dell'anno 2023, con riferimento alle competenze digitali di base, il nostro paese si colloca al 22° posto su 27 Stati membri dell'UE.

[31] Digital Economy and Society Index

Per rispondere alla domanda da cui siamo partiti, si afferma che al fine di avere un buon sistema di cyber security, è fondamentale costruire un impianto normativo solido e organico, allo stesso tempo è fondamentale la diffusione di programmi di sensibilizzazione e formazione, in quanto nessuna regola, per quanto rigorosa, potrà mai garantire la sicurezza se gli utenti non sono consapevoli dei rischi che le minacce informatiche possono causare.

Bibliografia e sitografia

[1] Wiener, 1948. Cybernetics or Control and Communication in the Animal and the Machine. Cambridge.

[2] Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici, Laboratorio Nazionale di Cybersecurity, Consorzio Interuniversitario Nazionale per l'Informatica, 2018.

[3] https://www.valorebf.it/qual-e-la-differenza-tra-information-security-e-cyber-security/

[4] https://www.fortinet.com/it/resources/cyberglossary/what-is-cybersecurity

[5] Rapporto Clusit 2024.

[6] Business Model 4.0 I modelli di business vincenti per le imprese italiane nella quarta rivoluzione industriale; Carlo Bagnoli, Alessia Bravin, Maurizio Massaro, Alessandra Vignotto; 2018.

[7] Report cost of data Breach 2024, IBM.

[8] Next Move Strategy Consulting; July 26, 2023; Size of cyber security market worldwide from 2021 to 2030.

[9] Gartner. October 13, 2022. Information security spending worldwide from 2017 to 2023, by segment.

[10] CompTIA. November 1, 2022. Most important cybersecurity areas worldwide in 2022 with a forecast until 2023

[11] Il Sole 24 Ore. February 23, 2023. Investments in the cybersecurity market in Italy from 2018 to 2022.

[12] Observatory Digital Innovation; February 23, 2022; Cybersecurity budget plan in Italy between 2018 and 2022.

[13] Imprese e ICT anno 2022, ISTAT, 4 Gennaio 2023.

[14] Cybersecurity Report 2023; Cybersecurity is much more than a matter of IT; Planetica.

[15] Kaspersky Lab e B2B International, Human factor main threats, 2024.

[16] Cybersecurity in Smart Factories; Capgemini, 2022.

[17] La sicurezza cibernetica delle imprese italiane: percezione dei rischi e pratiche di mitigazione; Banca d'Italia; 2022; Lorenzo Bencivelli e Matteo Mongardini

[18] De Gregorio, 2022, The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age, in Common Market Law Review.

[19] Maglio 2017, Cybersecurity e dati personali, in Maglio, Polini, Tilli, Manuale di diritto alla protezione dei dati personali.

[20] Contaldo, Peluso 2018, Cybersecurity. La nuova disciplina italiana ed europea alla luce della direttiva NIS. Pacini Editore.

[21] Salandri, Contaldo, 2016, La nuova disciplina giuridica cd. "orizzontale" della cybersicurezza per le infrastrutture in un'ottica di sviluppo dei sistemi, in Rivista amministrativa della Repubblica Italiana.

[22] Chiara 2023, Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali.

[23] Bavetta 2023. Direttiva NIS 2: verso un innalzamento dei livelli di cybersicurezza a livello europeo, in. Rivista di diritto dei media.

[24] Poletti 2023. La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica, in Rivista di diritto dei media.

[25] https://mondodigitale.aicanet.it/il-fattore-umano-e-la-regolazione-della-cybersecurity/