Politecnico di Torino

POLITECNICO DI TORINO

Corso di Laurea Magistrale In Ingegneria Gestionale (LM-31)

Tesi di Laurea Magistrale

Analisi degli investimenti in cybersecurity nelle imprese del settore privato italiano

Relatore:
Prof.ssa Laura Abrardi

Candidato:
Andrea Posca

Anno accademico 2022/2023

Abstract

Nel contesto attuale in cui le imprese possiedono e utilizzano una grande quantità di dati sensibili gioca un ruolo fondamentale la cybersecurity, attraverso gli investimenti per la prevenzione, la rilevazione e l'intervento tempestivo verso le minacce alla cybersicurezza. Questo studio, in primo luogo, si propone di indagare quali sono i fattori che determinano la scelta di un'impresa ad investire o meno nella sicurezza informatica. In secondo luogo, approfondisce quali sono i principali drivers che influenzano la probabilità di un'impresa di essere bersaglio di un attacco cibernetico. Infine, vuole ricercare quali sono i determinanti per cui un'organizzazione abbia più o meno consapevolezza di poter subire una violazione. Per rispondere a tali quesiti vengono utilizzati due campioni che fanno riferimento rispettivamente alle indagini svolte nel 2016 e nel 2022 da Banca d'Italia nei confronti delle imprese private italiane del settore industriale e dei servizi non finanziari. I risultati ottenuti con questo lavoro vogliono ampliare la ricerca svolta fino ad ora sul territorio italiano, suggerire quali interventi sono necessari per migliorare la condizione attuale e discutere le possibili strade da percorrere per le ricerche future.

In the current context where firms own and utilize a vast amount of sensitive data, cybersecurity plays a fundamental role through investments in prevention, detection, and timely response to cybersecurity threats. This study aims, firstly, to investigate the factors that determine a company's decision to invest in cybersecurity or not. Secondly, it explores the main drivers influencing the likelihood of a company becoming a target of a cyber-attack. Finally, it seeks to analyze the determinants for an organization to be more or less aware of the possibility of a breach. To address these questions, two samples are used, referring to surveys conducted in 2016 and 2022 by the Bank of Italy concerning private Italian companies in the industrial sector and non-financial services. The results obtained from this work aim to expand the research conducted so far in Italy, suggest necessary interventions to improve the current situation and discuss possible paths for future research.

Indice

Figure

Premessa e scopo del lavoro

Lo studio oggetto del presente lavoro riguarda uno degli argomenti più discussi degli ultimi anni, ovvero la *cybersecurity*, tema presente anche nel PNRR (Piano Nazionale di Ripresa e Resilienza). Il programma di investimenti, pari a 623 milioni di euro, ha l'obiettivo di rafforzare le difese informatiche per rendere più sicura la Pubblica Amministrazione, potenziando le capacità di monitoraggio, prevenzione e risposta a rischi e minacce *cyber*. La crescente diffusione della digitalizzazione nell'ambito dell'economia e della società, sebbene rappresenti un segno di progresso, comporta un aumento significativo dei pericoli e delle minacce di natura informatica in vari settori, come frodi, estorsioni informatiche e attacchi terroristici. Inoltre, le imprese dipendono sempre di più dai servizi software, e le reti complesse di valore digitale che coinvolgono enti pubblici, aziende statali e privati sono sempre più interconnesse. Questa interdipendenza aumenta considerevolmente il livello di rischio e sottolinea l'importanza cruciale di un'azione tempestiva ed efficace. La prevenzione e l'intervento immediato di fronte alle minacce informatiche sono fondamentali perché, a causa delle numerose interconnessioni tra le imprese, un incidente su una singola infrastruttura può diffondersi rapidamente a tutto il sistema[1]. Sono allora necessarie iniziative istituzionali avviate sia a livello nazionale che internazionale per rafforzare la *cyber resilience*, in modo da garantire la continuità nel funzionamento dei sistemi informativi prevenendo e gestendo le minacce informatiche.

Sullo sfondo delle crescenti tensioni internazionali e conflitti di alto profilo tra superpotenze ai confini dell'Europa, l'Italia ha registrato nel 2022 un totale di 188 attacchi hacker segnando un incremento del 169% rispetto al 2021[2]. Per fronteggiare tale minaccia, sembra che le imprese italiane si stiano muovendo nella direzione giusta, registrando una crescita degli investimenti in cybersicurezza del 18% nel 2022 raggiungendo il valore di 1,855 milioni di euro[3].

---

[1] Giannetto, B., & Fazio, A. (2022). *Cyber resilience per la continuità di servizio del sistema finanziario* (No. 18). Bank of Italy, Directorate General for Markets and Payment System.

[2] Clusit, 2023, "Rapporto Clusit 2023 sulla Sicurezza ICT in Italia"

[3] Cybersecurity360, & Osservatori Digital Innovation. (February 23, 2023). Market size of the cybersecurity sector in Italy from 2016 to 2022 (in million euros) [Graph]. In *Statista*. Retrieved October 11, 2023, from https://www-statista-com.ezproxy.biblio.polito.it/statistics/1055616/cybersecurity-market-size-italy/

L’obiettivo di tale ricerca è quello di indagare quali possono essere i fattori determinanti che guidano le scelte di investimento in cybersecurity delle imprese italiane private del settore industriale e dei servizi attraverso l’utilizzo di tecniche econometriche, in particolare dell’analisi di regressione Ordinary Least Square (OLS).

Lo studio espone nel Capitolo 1 le definizioni del termine Cybersecurity e una introduzione sul contesto attuale sia a livello globale che in Italia sugli investimenti effettuati in sicurezza informatica, riportando anche le relative iniziative nazionali e interventi di policy. Viene fatto anche un breve approfondimento sulle tipologie principali di attacchi informatici e la loro diffusione. Il Capitolo 2, invece, consiste nell’analisi della letteratura economica fino ad oggi presente inerente a studi effettuati sugli investimenti delle imprese in cybersicurezza e sull’individuazione delle variabili indipendenti che possono determinare l’ammontare di tali investimenti, del rischio informatico delle imprese e dei costi dovuti alle minacce cyber. Si procede successivamente nel Capitolo 3 all’analisi descrittiva effettuata sui dati dei campioni ottenuti dalle indagini conseguite dalla Banca d’Italia nel 2016 e nel 2022, che sono gli anni in cui uno degli argomenti centrali dei questionari sottoposti alle imprese è stato appunto la cybersecurity, dedicando una sezione di domande specifica.

In seguito, nel capitolo 4 si presentano i modelli di regressione Ordinary Least Square (OLS) e si riassumono i risultati della ricerca e, infine, nel capitolo 5, sono riportate le conclusioni per suggerire quali interventi sono necessari per migliorare la condizione attuale.

1. Introduzione

1.1 Definizione di Cybersecurity

Negli ultimi anni il termine “Cybersecurity” è stato molto usato ed è stato oggetto di dibattito nella ricerca di una definizione completa e accettabile in grado di catturare la multidimensionalità del tema. A proposito della natura multidisciplinare del termine, Fredrick Chang [1], ex direttore della ricerca presso la National Security Agency degli Stati Uniti, parla della cybersicurezza: *“A science of cybersecurity offers many opportunities for advances based on a multidisciplinary approach, because, after all, cybersecurity is fundamentally about an adversarial engagement. Humans must defend machines that are attacked by other humans using machines. So, in addition to the critical traditional fields of computer science, electrical engineering, and mathematics, perspectives from other fields are needed”.* L’assenza di una definizione unica e condivisa può limitare le opportunità di progresso della cybersicurezza, che richiedono il contributo di diversi campi di studio, oltre all'informatica, all'ingegneria elettrica e alla matematica, in modo che collaborino per affrontare le sfide della cybersecurity. Anche la valutazione dell'ENISA [2], intitolata "Definition of Cyber security - Gaps and overlaps in standardisation", conclude che: *“There does not need to be a definition for Cybersecurity, in the conventional sense that we tend to apply to definitions for simple things, like the authentication of an identity (a security mechanism allowing the verification of the provided identity). The problem is that Cybersecurity is an enveloping term; and it is not possible to make a definition to cover the extent of the things Cybersecurity covers”*.

La terminologia utilizzata per discutere gli aspetti della sicurezza dei dispositivi e delle informazioni digitali è cambiata notevolmente negli ultimi anni [3]. All'inizio del secolo, i termini regolarmente utilizzati in questo contesto erano "Computer Security", "IT Security" o "Information Security". Tuttavia, verso la fine del primo decennio, una nuova terminologia ha iniziato a diventare sempre più popolare con l'uso del termine "Cyber Security". Il termine era già in uso negli anni precedenti, ma la sua popolarità è aumentata notevolmente quando il Presidente degli Stati Uniti Barack Obama, nel 2009, ha proclamato: *"I call upon the people of the United States to recognize the importance of cybersecurity and to observe this month with appropriate activities, events, and trainings to enhance our national security and resilience"* [4]. L'impatto immediato di questo comunicato stampa sulla terminologia può essere illustrato con l'aiuto delle tendenze di ricerca di Google che mostrano un picco notevole in questo periodo (Figura 1). Le linee di tendenza del grafico mostrano le ricerche

totali di un termine rispetto al numero totale di ricerche effettuate su Google nel corso del tempo.

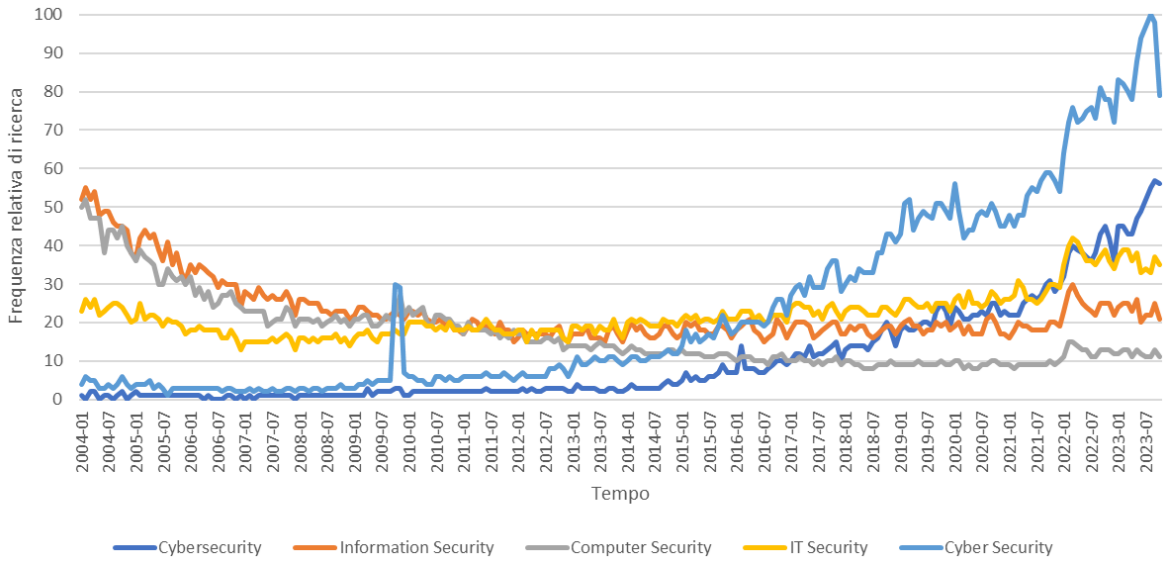

Figura 1. Frequenza relativa di ricerca dei termini inerenti alla "Security" su Google nel 2004-2023

Il termine Cybersecurity può essere trovato scritto in modo congiunto o disgiunto e, osservando le tendenze di ricerca illustrate, si nota che entrambi i termini hanno una tendenza all'aumento; tuttavia, la versione disgiunta (Cyber Security) mostra una prevalenza in numeri assoluti ed è la grafia che verrà utilizzata in futuro.

In prima battuta, il termine può essere scomposto in "Cyber" e "Security" per definire i due domini principali. Secondo l'Oxford English Dictionary, "Cyber" è tipicamente un prefisso che coinvolge la cultura di computer, realtà virtuale, o internet [5]. Riguarda dunque tutto ciò che fa parte del Cyberspazio, termine reso popolare dal romanzo di William Gibson nel 1984, Neuromante, in cui viene descritto come uno spazio tridimensionale di pura informazione che si muove tra computer e cluster di computer in cui le persone sono generatori e utenti dell'informazione. Oggi è considerato in modo più ampio e, ad esempio, Public Safety Canada [6] definisce il cyberspazio come *"the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where…people are linked together to exchange ideas, services and friendship"*. Come sottolineato da Deibert e Rohozinski [7] ha una natura dinamica in continua evoluzione con più livelli di infrastrutture fisiche, software, di regolamenti, idee, innovazioni e interazioni umane.

Oltre ad essere il prefisso di "Security", il termine "Cyber" si ritrova spesso trattando di rischio (Cyber Risk) e di relative minacce (Cyber Threat) le cui definizioni rispettive, in

riferimento al Cyber Lexicon di FBS (2023) [8], sono "*The combination of the probability of cyber incidents occurring and their impact*" e "*A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber security*".

Il termine "Security" è difficile da definire in senso generale perché dipende dal contesto in cui è applicato e dalla prospettiva che si assume. Secondo Buzan, Wæver e Wilde [9], i discorsi sulla sicurezza includono e cercano necessariamente di capire chi mette in sicurezza, su quali questioni (minacce), per chi (l'oggetto referente), perché, con quali risultati e in quali condizioni (la struttura). Il principio generale, definito nell'Oxford English Dictionary [5], è che la sicurezza è lo stato in cui si è liberi da pericoli o minacce, ovvero essere protetti o non esposti al pericolo.

Andando ad analizzare la letteratura passata, si osserva come le differenti definizioni siano legate al contesto di interesse, spesso soggettive e poco informative. Le discipline accademiche che hanno trattato il termine "Cybersecurity" sono svariate: oltre alle più comuni come ingegneria, tecnologia, informatica, sicurezza e difesa, si possono trovare studi politici, psicologia, istruzione, sociologia e diritto. Di seguito sono riportate le definizioni principali che possono fornire un quadro generale delle diverse prospettive:

1. *"Cybersecurity consists largely of defensive methods used to detect and thwart would-be intruders."* (Kemmerer, 2003) [10]
2. *"Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption."* (Lewis, 2006) [11]
3. *"Cyber Security involves reducing the risk of malicious attack to software, computers and networks. This includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on."* (Amoroso, 2006) [12]
4. *"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets."* (ITU, 2009) [13]
5. *"Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."* (CNSS, 2015) [14]

6. *“The body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability.”* (Public Safety Canada, 2012) [15]

7. *“The art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, assets and critical infrastructure.”* (Canongia & Mandarino, 2014) [16]

8. *“The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.”* (Oxford University Press, 2014) [17]

9. *“The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.”* (DHS, 2014) [18]

10. *“Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights.”* (Craigen, Diakun-Thibault, Purse, 2014) [19]

11. *"Cybersecurity is the collection and concerting of resources including personnel and infrastructure, structures, and processes to protect networks and cyber- enabled computer systems from events that compromise the integrity and interfere with property rights, resulting in some extent of loss."* (Schiliro, 2023) [20]

12. *“Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.”* (Cyber Lexicon di FBS, 2023) [8]

Gli autori Craigen, Diakun-Thibault e Purse [19] hanno identificato cinque temi dominanti della cybersecurity, utili per formare un contesto critico al processo di definizione del termine: i) soluzioni tecnologiche, ii) eventi, iii) strategie, processi e metodi, iv) impegno umano, e v) oggetti di riferimento (della sicurezza). Inoltre, la cybersecurity si distingue per:

- la sua natura sociotecnica che coinvolge diverse discipline;
- la sua struttura priva di scala, in cui gli attori della rete hanno capacità potenzialmente simili;
- l'elevato livello di cambiamento, connessione e velocità di interazione.

È importante articolare una definizione concisa, inclusiva, significativa e unificante per portare a una maggiore comprensione e collaborazione necessarie per affrontare le crescenti e complesse minacce al cyberspazio e, inoltre, per influenzare gli approcci delle università, delle industrie e delle organizzazioni governative e non governative alle sfide della cybersecurity.

Ma la Cybersecurity e la Information Security (sicurezza dell'informazione) sono la stessa cosa? A questa domanda hanno cercato di rispondere Von Solms e Van Niekerk [21] sostenendo che, quando la tecnologia utilizza il cyberspazio, i danni risultati rientrano nel campo della cybersecurity. Quindi, la sicurezza dell'informazione e la cybersecurity si sovrappongono parzialmente, con i danni conseguenti che fanno parte della cybersecurity, ma non necessariamente della sicurezza dell'informazione. Definire chiaramente la relazione tra cybersecurity e sicurezza delle informazioni è utile per riuscire a distinguere le relative governance e responsabilità all'interno delle organizzazioni. Il messaggio centrale dello studio di Basie von Solms e Rossouw von Solms [22] è che la cybersecurity è un sottoinsieme della sicurezza delle informazioni e, di conseguenza, la governance della cybersecurity è un sottoinsieme della governance della sicurezza delle informazioni. La base di questa argomentazione deriva dalla norma ISO/IEC 27032:2012 [23], documento creato dall'Organizzazione Internazionale per la Standardizzazione e dalla Commissione Elettrotecnica Internazionale nel 2012, che definisce la Cybersecurity come *"preservation of the confidentiality, integrity and availability of information in Cyberspace"*. D'altro canto, la norma ISO/IEC 27000:2018 [24] definisce la sicurezza delle informazioni come *"preservation of the confidentiality, integrity and availability of information"*. Pertanto, la distinzione tra cybersecurity e sicurezza delle informazioni risiede nel fatto che la cybersecurity si concentra esclusivamente sulla protezione delle informazioni nel cyberspazio, mentre la sicurezza delle informazioni si estende alla protezione delle informazioni in qualsiasi contesto o ambiente. Oggi lo standard rispetto al termine Cybersecurity è stato aggiornato alla norma ISO/IEC 27032:2023 [25] che lo definisce come *"safeguarding of people, society, organizations and nations from cyber risks"*. L'ISACA[4] ha creato il "Cybersecurity Fundamentals Certificate", come certificato professionale entry-

[4] Leader riconosciuto a livello mondiale nel settore IS/IT da oltre 50 anni, ISACA è un'organizzazione professionale impegnata a promuovere la fiducia digitale, consentendo ai professionisti IS/IT di accrescere le proprie competenze e conoscenze in materia di audit, cybersecurity, tecnologie emergenti e altro ancora.

level nel campo della cybersecurity e per la preparazione al fine di ottenere tale certificazione fornisce la guida "The ISACA CSx Cybersecurity Fundamentals Study Guide" [26], che afferma: *"[. . .] but in reality cybersecurity is a part of information security."* e continua: *"Information security deals with information, regardless of its format–it encompasses paper documents, digital and intellectual property in people's minds, and verbal or visual communications. Cybersecurity, on the other hand, is concerned with protecting digital assets–everything from networks to hardware and information that is processed, stored or transported by internetworked information systems. Additionally, concepts such as nation-state-sponsored attacks and advanced persistent threats (APTs) belong almost exclusively to cybersecurity. It is helpful to think of cybersecurity as a component of information security"*. Questa guida allo studio definisce la cybersecurity *"as protecting information assets by addressing the threats to information processed, stored and transported by internetworked information systems"*. Quindi, anche in questa guida si sottolinea come sia corretto pensare la cybersecurity come un sottocomponente della sicurezza delle informazioni. La Figura 2 permette di avere una visione grafica ad insiemi della relazione tra la cybersecurity gli altri domini di sicurezza.

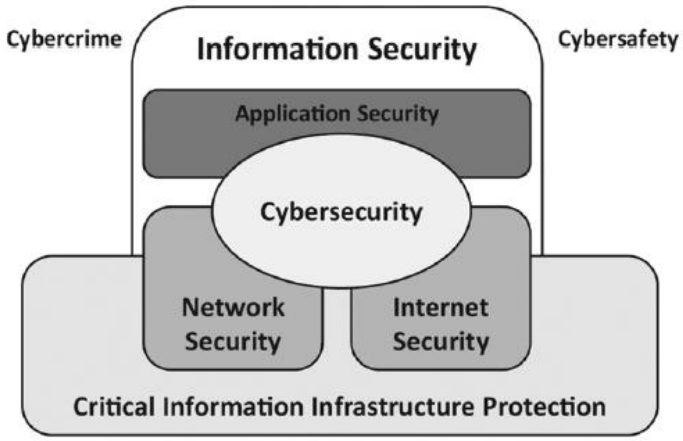

Figura 2. Relazione tra cybersecurity e altri domini di sicurezza [22]

Dopo aver analizzato la differenza tra Cybersecurity e Information Security, possiamo andare a definire le relative governance. Lo standard internazionale ISO/IEC 27014:2013 [27] afferma che la governance della sicurezza delle informazioni è *"system by which an organisation's information security activities are directed and controlled"* . Abbiamo visto come la cybersecurity è "limitata" agli asset informativi digitali che potrebbero essere compromessi attraverso l'uso di internet. Pertanto, la spiegazione della governance della cybersecurity di Basie von Solms e Rossouw von Solms [22] è: *"Cyber Security Governance, as part of Information Security Governance, is the process of directing and*

controlling the protection of a company's digital information assets from the risks that are related to using the internet". Questa affermazione fa riflettere sull'utilizzo di Internet da parte di una impresa: più la dipendenza da Internet è elevata, tanto più è grande la minaccia informatica e tanto più devono essere grandi gli sforzi e gli investimenti in cybersecurity.
Nelle definizioni fino ad ora osservate emergono frequenti i concetti di confidenzialità, integrità e disponibilità. Questi compongono la cosiddetta triade CIA (Confidentiality, Integrity, Availability) introdotta nel rapporto Anderson [28] e ripetuta in Saltzer e Schroeder [29], ma coniata successivamente da Steve Lipner intorno al 1986 [30]. Il principio che sta alla base della triade è che la cybersecurity si basa su tre aspetti fondamentali [31]:

- Confidenzialità, ovvero che soggetti non autorizzati non possano utilizzare o non possano avere accesso a dati e risorse sensibili lungo tutto il ciclo di vita, a partire dall'immagazzinamento, durante l'utilizzo o il transito nella rete.
- Integrità, ovvero la capacità di garantire che i dati e le risorse non vengano in alcun modo modificate o cancellate mantenendo la loro veridicità.
- Disponibilità, ovvero garantire la possibilità per i soggetti autorizzati di accedere ai dati o alle risorse di cui hanno bisogno per il tempo necessario, anche in modo ininterrotto.

Questo approccio non può più funzionare nel contesto di oggi, in cui i dispositivi che utilizziamo sono costantemente connessi tra loro e i processi del mondo fisico dipendono nella maggior parte da computer. Non si può guardare a questi aspetti come misure binarie per cui in un certo momento sono veri o falsi e soprattutto lo stato attuale non dà alcuna garanzia per il futuro [32]. Con l'avvento dei dispositivi mobili si sono resi necessari nuovi approcci alla cybersecurity e tra questi troviamo il NIST Cybersecurity Framework [33], definito come un insieme di cinque attività, che vanno svolte non in modo seriale ma piuttosto in modo concomitante e continuo per formare una cultura operativa che affronti il rischio dinamico della cybersecurity:

- Identificare: sviluppare una comprensione organizzativa per gestire il rischio di cybersecurity per sistemi, persone, beni, dati e capacità.
- Proteggere: sviluppare e implementare adeguate misure di salvaguardia per garantire la fornitura di servizi critici.
- Rilevare: sviluppare e implementare attività appropriate per identificare il verificarsi di un evento di cybersecurity.

- Rispondere: sviluppare e implementare attività appropriate per intervenire in caso di incidente di cybersecurity rilevato.
- Recuperare: sviluppare e implementare attività appropriate per mantenere i piani di resilienza e per ripristinare qualsiasi capacità o servizio che sia stato compromesso a causa di un incidente di cybersecurity.

L'attività di identificazione vuole individuare gli asset di un'organizzazione che devono essere messi in sicurezza ed esaminare il contesto in cui si trovano. La protezione non è l'obiettivo principale ma è solo una delle attività previste inserendo le misure di sicurezza in una prospettiva più ampia. Rilevazione, risposta e recupero permettono di vedere la cybersecurity non in maniera statica ma dinamica, considerando il fatto che alcuni rischi sono troppo costosi da proteggere ed è quindi necessario adottare diverse misure per mitigare le conseguenze. Questo significa che la cybersicurezza non può essere un obiettivo assoluto, ma deve essere vista come un'attività continua che si inserisce in un determinato contesto.

1.2 Tipologie di attacchi informatici e diffusione nel mondo e in Italia

Oltre alla comprensione del termine Cybersecurity, è importante avere una panoramica delle minacce e delle tipologie di attacchi informatici che si possono subire. Gli attacchi informatici si possono distinguere in base all'effetto che l'hacker vuole ottenere sul soggetto colpito. IBM [34], azienda statunitense leader nel settore informatico, definisce un cyberattacco come *"A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, applications or other assets through unauthorized access to a network, computer system or digital device"* e individua alcune minacce comuni alla sicurezza informatica che si stanno diffondendo e che non vanno a colpire solo le organizzazioni direttamente, ma anche gli ambienti per il lavoro da casa, gli strumenti di accesso remoto e i nuovi servizi cloud [35]. Il *malware*, che è l'abbreviazione di "software dannoso", è tra i tipi di violazioni informatiche più frequenti. Si tratta di qualsiasi codice software o programma per computer creato per danneggiare intenzionalmente un sistema informatico o i suoi utenti, permettendo di ottenere l'accesso non autorizzato a dati sensibili, dirottare, interrompere o danneggiare sistemi informatici o gestirli da remoto, tenere in ostaggio dati o sistemi chiedendo in cambio grandi somme di denaro. Questo ultimo caso riguarda nello specifico il *ransomware*, che è un tipo di malware che può crittografare i dati o i sistemi di una vittima fino a quando non paga un riscatto. L'aggressore può, inoltre, richiedere un secondo riscatto per impedire la condivisione o la pubblicazione dei dati delle vittime (in questo caso di parla di attacco a doppia estorsione). I tipici messaggi, e-mail, telefonate,

richieste di cambiare password o di inserire i dati della carta di credito che provengono apparentemente da grandi marchi e che cercano di indurre l'utente a scaricare malware fanno parte degli attacchi di *phishing*. Il phishing rientra tra i tipi di "Ingegneria sociale" che comprende una serie di tecniche in grado di manipolare le persone affinché condividano informazioni, scarichino software o visitino siti web che non dovrebbero, andando a sfruttare la debolezza umana piuttosto che quella dei sistemi informatici (per questo viene definita anche *human hacking*). In molti pensano che le minacce informatiche provengano solo dall'esterno, ma in realtà possono provenire anche da utenti interni alle organizzazioni che abusano del loro accesso autorizzato per violare la sicurezza e tra questi, secondo uno studio recente, il 44% sono attori malintenzionati che hanno comportato un costo medio per incidente nel 2022 di 648.062 dollari [36]. Questa categoria rientra tra i tipi di attori che compiono attacchi informatici che vedremo successivamente ma, allo stesso tempo, è anche un metodo per danneggiare un sistema informativo. Un altro studio ha rilevato che mentre la minaccia esterna media compromette circa 200 milioni di record, gli incidenti che coinvolgono un attore interno hanno portato all'esposizione di 1 miliardo di record o più [37]. Un altro tipo di minaccia informatica è quella degli attacchi *DDoS (Distributed Denial of Service),* che mirano a interrompere il corretto funzionamento di un server, di un sito web o di una rete sovraccaricandoli di traffico attraverso una rete di sistemi multipli distribuiti dirottati da remoto utilizzando un malware.

Oltre a questi tipi di attacchi informatici possiamo trovare i *Cross-site scripting (XSS),* che inseriscono un codice dannoso in una pagina web o in un'applicazione che viene eseguito autonomamente quando un utente fa visita al sito o applicazione rubando informazioni sensibili o reindirizzando l'utente a un sito dannoso. Ci sono poi attacchi che utilizzando il linguaggio SQL (Structured Query Language) per inviare comandi dannosi al database di backend di un sito inseriti attraverso i campi rivolti all'utente (per questo chiamati *SQL injection)*, come le barre di ricerca e le finestre di login, e che inducono a restituire dati privati come numeri di carte di credito o dettagli dei clienti. Gli *adware* sono dei programmi progettati per mostrare messaggi pubblicitari nella pagine di servizi online e programmi gratuiti e, nel caso di pubblicità illegittime, possono portare a siti sospetti o all'installazione inconsapevole di malware e virus. Quando navighiamo nel web ci viene spesso chiesto il consenso ai cosiddetti *cookie* che sono dei piccoli file di testo che contengono informazioni relative al modo di interagire con un determinato sito web e vengono inviati da un sito al computer dell'utente che lo visita per migliorare l'esperienza di navigazione. Nonostante

abbiano uno scopo innocuo di identificazione e profilazione dell'utente, un hacker può essere in grado di sfruttare alcune vulnerabilità dei siti per intercettare questi cookie e utilizzarli per impersonare l'utente, riuscendo ad appropriarsi di account e credenziali di accesso, senza che né l'utente né il sito o servizio se ne accorgano. Sentiamo spesso il consiglio di collegarci a reti Wi-Fi che conosciamo e che siano sicure per evitare di essere vittime di *sniffing,* ovvero una tecnica che permette di intercettare i dati che si muovono in una rete permettendo all'hacker di collegarsi in una rete non ben protetta e di avere poi l'accesso ai dispositivi connessi [38].

Facendo riferimento agli incidenti dolosi, la tassonomia ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) stabilita dal MITRE nel 2013 permette di classificare il comportamento dei cyber attaccanti e fornire un quadro comune per l'attacco e la difesa [39]. Sono individuate 12 fasi, chiamate "tattiche", che un attaccante seguirebbe per infiltrarsi e distruggere un sistema informatico e ciascuna fase ha una propria definizione consolidata (Figura 3).

1	Initial Access	Techniques that use various entry vectors to gain their initial foothold within a network (include targeted spearphishing and exploiting weaknesses on public-facing web servers).
2	Execution	The adversary is trying to run malicious code. Execution consists of techniques that result in adversary-controlled code running on a local or remote system.
3	Persistence	Techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.
4	Privilege Escalation	Techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities.
5	Defense Evasion	Techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware.
6	Credential Access	Techniques for stealing credentials like account names and passwords, such as keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.
7	Discovery	Techniques that an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act. They also allow adversaries to explore what they can control and what's around their entry point in order to discover how it could benefit their current objective. Native operating system tools are often used toward this post-compromise information-gathering objective
8	Lateral Movement	Techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it. Reaching their objective often involves pivoting through multiple systems and accounts to gain.
9	Collection	Techniques that adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives.
10	Command and Control	Techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection.
11	Exfiltration	Techniques that adversaries may use to steal data from your network. Once they have ve collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over their command and control channel or an alternate channel.
12	Impact	Techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. Techniques used for impact can include destroying or tampering with data. In some cases, business processes can look fine, but may have been altered to benefit the adversaries' goals. Adversaries might use these techniques to achieve their final goal or to cover up a breach of confidentiality.

Figura 3. Le 12 tattiche ATT&CK di MITRE con definizione [39]

Oltre ad esserci diversi tipi di attacchi informatici, esistono anche diverse categorie di attori che compiono gli attacchi. Questi possono avere attributi, motivazioni, abilità e tattiche diverse [40]. Oggi è possibile distinguere gli hacktivisti, gli attori nation-state, i cybercriminali, i *thrill seekers*, gli attori interni alle organizzazioni e i cyberterroristi. L'importanza della comprensione dei diversi tipi di attaccanti è concreta perché aiuta a migliorare la sicurezza informatica individuale e collettiva. Nella Tabella 1 possiamo trovare le caratteristiche dei principali tipi di attori.

Cybercriminals	Questi criminali informatici o gruppi commettono delitti online, spesso con l'intento di guadagnare. Tra i loro reati più diffusi ci sono gli attacchi ransomware e le truffe di phishing, che ingannano le persone per farle effettuare trasferimenti di denaro o rivelare informazioni sensibili come dati delle carte di credito, credenziali di accesso, proprietà intellettuale e altre informazioni private.
Nation-state actors	I governi e gli Stati nazionali forniscono frequentemente finanziamenti agli agenti delle minacce con l'intento di sottrarre dati delicati, raccogliere informazioni confidenziali o sabotare le infrastrutture critiche di un altro governo. Queste operazioni dannose coinvolgono spesso spionaggio o attacchi informatici, e solitamente sono finanziati in modo sostanzioso, rendendo così le minacce intricate e ardue da individuare.
Hacktivists	Questi individui impegnati in attività minacciose utilizzano metodi di hacking per sostenere cause politiche o sociali, come la promozione della libertà di espressione o l'esposizione di violazioni dei diritti umani. Gli hacktivisti credono di agire per favorire un cambiamento sociale positivo e ritengono giustificato mirare a singoli individui, organizzazioni o istituzioni governative per rivelare segreti o altre informazioni confidenziali. Un esempio noto di gruppo hacktivista è Anonymous, un collettivo internazionale di hacker che afferma di difendere la libertà di espressione su Internet.
Thrill seekers	Gli amanti del brivido, proprio come sembra, sono individui che si dedicano all'hacking di sistemi informatici e alla manipolazione di dati principalmente per il proprio divertimento. Alcuni di loro si sfidano a rubare quante più informazioni sensibili possibile, mentre altri utilizzano l'hacking come un mezzo per approfondire la comprensione del funzionamento delle reti e dei sistemi informatici. Tra questi, esiste una categoria di persone chiamata "script kiddies," che non possiedono competenze tecniche avanzate ma sfruttano strumenti e tecniche preesistenti per attaccare sistemi vulnerabili, principalmente per il proprio divertimento o soddisfazione personale. Anche se non sempre intendono causare danni, gli amanti del brivido possono involontariamente provocare danni interferendo con la sicurezza informatica di una rete e aprendo la strada a futuri attacchi informatici.
Insider threats	A differenza di molti altri attori, gli individui interni con potenziale minaccia non agiscono sempre con cattive intenzioni. Alcuni danni aziendali possono derivare da errori umani, come l'installazione involontaria di malware o la perdita accidentale di dispositivi aziendali, che potrebbero essere poi utilizzati da criminali informatici per accedere alla rete. Tuttavia, ci sono anche insider malintenzionati, come i dipendenti insoddisfatti che abusano dei privilegi di accesso per rubare dati a scopo di lucro o danneggiare dati e applicazioni come vendetta per motivi di lavoro.
Cyberterrorists	I cyberterroristi muovono attacchi informatici con motivazioni politiche o ideologiche che possono minacciare o incitare alla violenza. Questi individui

	possono appartenere a Stati nazionali, agire come individui indipendenti o essere parte di gruppi non governativi.

Tabella 1. Tipologie di attori degli attacchi informatici

Questa panoramica può far comprendere come i cyberattacchi possano interrompere, danneggiare o persino distruggere un'azienda. Più l'impresa possiede dati sensibili o risorse digitali e più il danno economico causato da una violazione informatica è alto. Come riportato nel report "Cost of a Data Breach Report 2023" di IBM [41], il 2023 vede il costo medio di una violazione dei dati ai massimi storici raggiungendo i 4,45 milioni di dollari, un aumento del 2,3% rispetto ai 4,35 milioni del 2022. In una prospettiva a lungo termine, il costo medio è aumentato del 15,3% rispetto ai 3,86 milioni del report 2020. Questo costo è composto da diversi elementi, che possono essere il costo di rilevazione e risposta alla violazione, i tempi di inattività e i relativi mancati guadagni, il costo dell'eventuale riscatto richiesto dall'attaccante e, considerati i più difficili di cui rientrare, i danni di lungo termine alla reputazione e al marchio dell'azienda.

Cerchiamo ora di dare una panoramica sull'andamento e sulle caratteristiche principali degli attacchi informatici a livello globale e in Italia. Secondo il rapporto redatto dal Clusit [42] emerge che a livello mondiale nel 2022 la crescita degli attacchi informatici è del 21% rispetto al 2021, mentre in Italia del 169% (Figura 4), dato che dovrebbe far riflettere sull'importanza delle misure di difesa informatica adottate e da adottare al più presto. L'anno 2022 si caratterizza come il peggiore da sempre per la cybersecurity registrando 2.489 incidenti gravi a livello globale, con il 7,6% andato a segno nel nostro Paese.

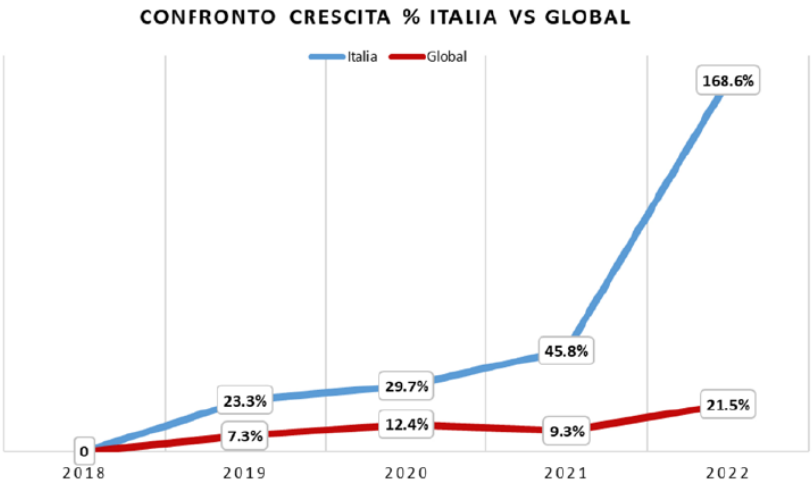

Figura 4. Crescita percentuale degli attacchi Italia vs. Mondo 2018-2022 [42]

Nel corso del 2022, oltre ad aumentare in numero, gli attacchi informatici su scala globale hanno anche intensificato la loro gravità. In circa l'80% dei casi, questi attacchi hanno raggiunto livelli di impatto elevato o critico. Questo dato è coerente con la situazione italiana, dove tali attacchi hanno avuto conseguenze significative per le vittime in termini di reputazione, impatto economico, sociale e geopolitico. L'analisi degli eventi di cybersecurity noti nel 2022 mette in luce una chiara predominanza di attacchi con scopi legati al cybercrime. A livello globale, questi attacchi hanno superato i 2.000 casi, rappresentando l'82% del totale, con un aumento del 15% rispetto al 2021 (Figura 5). In Italia, questa percentuale raggiunge il 93%, registrando una crescita del 150% rispetto all'anno precedente. Questa categoria di attacchi, connotata da gravi implicazioni economiche dovute alla diffusione degli attacchi ransomware, ha mostrato una costante tendenza al rialzo negli ultimi cinque anni. In termini assoluti, anche gli attacchi associati a spionaggio e sabotaggio (10% del totale), guerra dell'informazione (4% del totale) e azioni di attivismo (3% del totale) hanno raggiunto il loro apice storico a livello globale nel 2022, principalmente a causa del conflitto europeo.

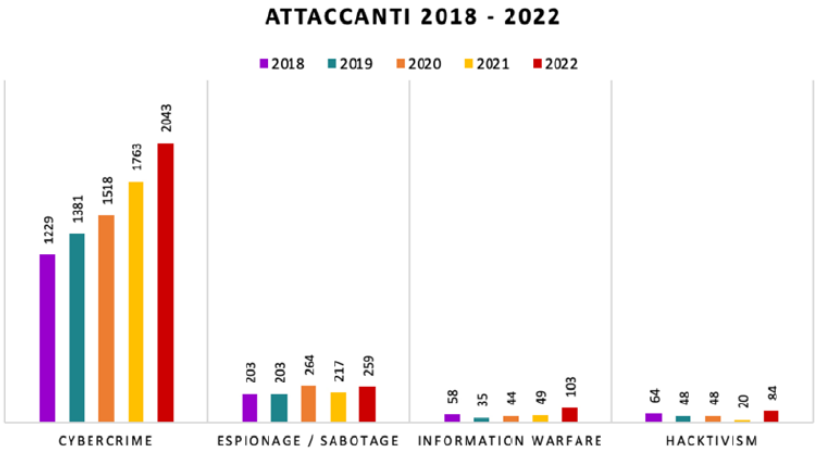

Figura 5. Distribuzione degli attaccanti a livello globale 2018-2022 [42]

La maggior parte degli attacchi noti in Italia appartiene alla categoria "Cybercrime," che costituisce il 93% del totale degli attacchi nel paese (Figura 6). Questo valore è superiore del 11% rispetto alla media globale. Gli incidenti classificati come "Hacktivism" costituiscono il 7% del totale, mentre non sono stati rilevati attacchi significativi nelle categorie "Espionage / Sabotage" o "Information Warfare."

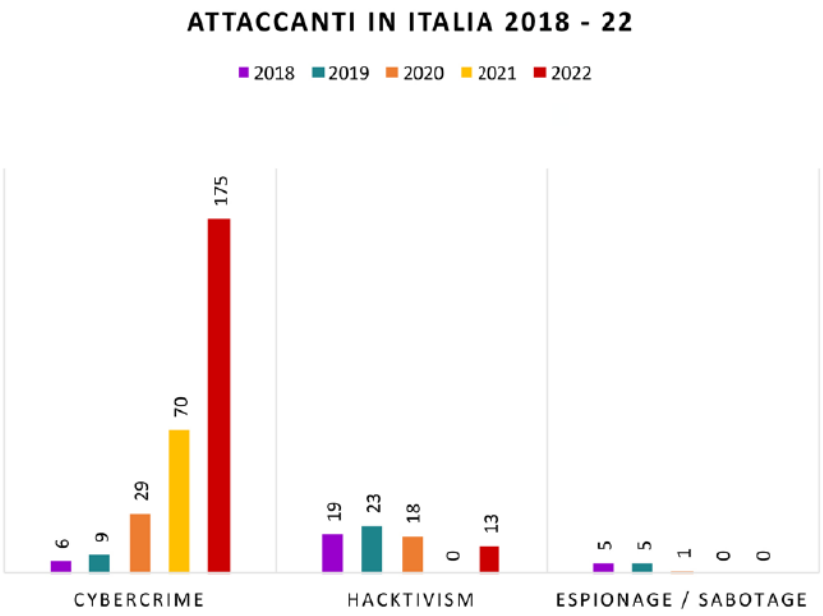

Figura 6. Attaccanti in Italia 2018-2022 [42]

Ma quali sono i settori più colpiti? A livello globale, le principali vittime sono i "Multiple Targets" (22%), con un aumento del 97% rispetto al 2021, che rappresentano campagne di attacco non mirate che continuano a generare impatti significativi. Al secondo posto si trova il settore governativo e delle pubbliche amministrazioni (12%), che, come indicato dai ricercatori di Clusit, ha registrato un aumento complessivo del 25% nell'arco di cinque anni. Nel 2022, il 12% degli attacchi è stato indirizzato verso il settore sanitario, registrando un aumento percentuale del 16% rispetto al 2021. L'11% degli attacchi ha colpito l'industria informatica e l'8% ha preso di mira il settore scolastico e universitario. Sono aumentati in percentuale gli attacchi contro il settore finanziario-assicurativo (+40%) e il settore manifatturiero, che ha visto gli attacchi raddoppiati dal 2018 e con una crescita del 79% dal 2021. Questo aumento è probabilmente dovuto alla diffusione sempre maggiore dell'Internet delle cose (IoT) e alla tendenza all'interconnessione dei sistemi industriali, spesso insufficientemente protetti. Anche nel settore delle notizie e dei media si è verificato un raddoppio tra il 2020 e il 2022, registrando una crescita del 70% dal 2021. Questo aumento è in parte attribuibile al conflitto in Ucraina, con attività di disinformazione, propaganda e interruzione dei media considerati nemici da colpire.

In Italia nel 2022, il settore più colpito è stato quello governativo, con il 20% degli attacchi, seguito a breve distanza dal settore manifatturiero (19%), che rappresenta il 27% del totale degli attacchi censiti a livello globale nel settore (Figura 7).

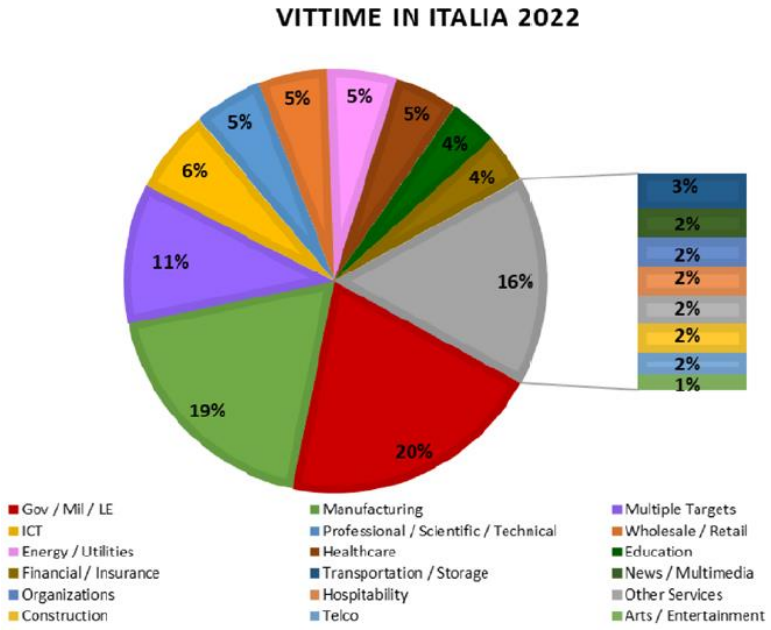

Figura 7. Distribuzione delle vittime in Italia nel 2022 [42]

L'analisi delle metodologie di attacco contribuisce a spiegare le ragioni dietro l'aumento significativo degli attacchi subiti dalle nostre imprese e istituzioni. Il malware domina, come nel contesto globale, ma in Italia la sua presenza è notevolmente più marcata (53%, con un aumento del 6% rispetto alla media mondiale). I casi di phishing e ingegneria sociale, sebbene meno diffusi in Italia rispetto al resto del mondo, sono stati meno rilevanti (8% contro il 12% globale). Gli attacchi DDoS aumentano leggermente e rimangono sostanzialmente stabili rispetto agli anni precedenti (4%, in linea con la media globale, contro il 6% dell'anno precedente). Infine, è importante sottolineare il numero significativo di situazioni in cui non è possibile identificare la tecnica primaria dell'attacco (sconosciuto, 27% rispetto al 24% globale), evidenziando una mancanza nella capacità di individuare il tipo specifico di attacco (Figura 8).

Le tecniche legate ai malware sono quasi sempre standardizzate e sono il risultato dell'industria del cyber-crime che rappresenta la principale fonte di attività malevole nel nostro Paese. Questo suggerisce l'ipotesi che l'incremento degli attacchi in Italia sia correlato ai gravi limiti nelle capacità di difesa delle vittime. La percentuale di incidenti derivanti da vulnerabilità già note potrebbe facilmente diminuire se le organizzazioni adottassero processi efficaci di gestione delle vulnerabilità e di aggiornamento della sicurezza. Nonostante ciò, la situazione in Italia non è così negativa come nel resto del mondo, visto che la percentuale è la metà di quella globale (6% contro il 12%).

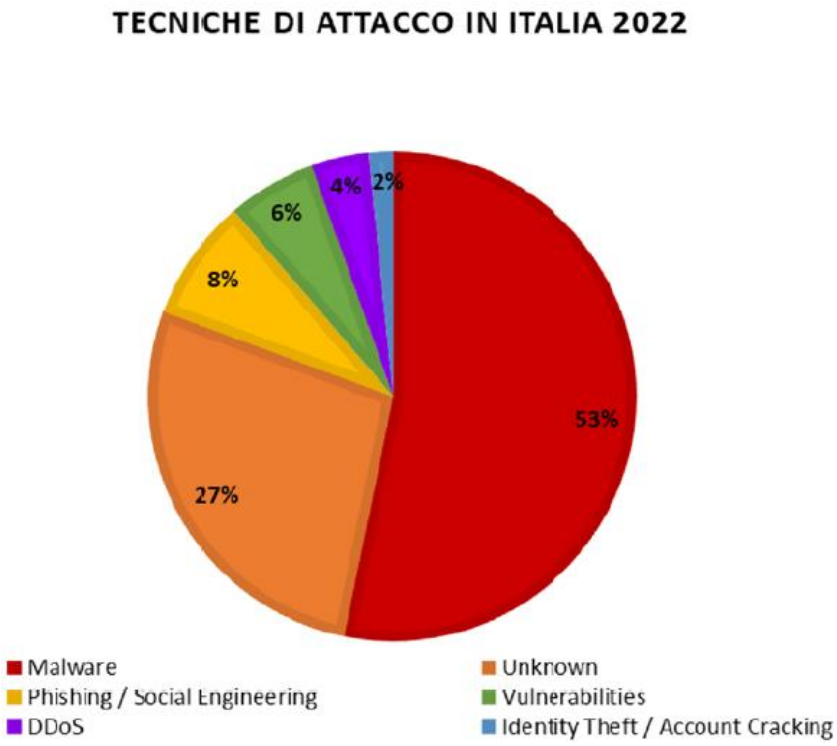

Figura 8. Tecniche di attacco in Italia nel 2022 [42]

1.3 Investimenti in sicurezza informatica nel contesto globale e italiano

Così come sono in crescita gli attacchi informatici, anche gli investimenti nelle misure di protezione informatica sono in un trend crescente negli ultimi anni per far fronte alle minacce (Figura 9). Secondo Next Move Strategy Consulting, il mercato globale della cybersecurity è valutato 222 miliardi di dollari nel 2022 e si stima che raggiunga 657 miliardi di dollari nel 2030, con un CAGR del 12,8% dal 2022 al 2030 [43].

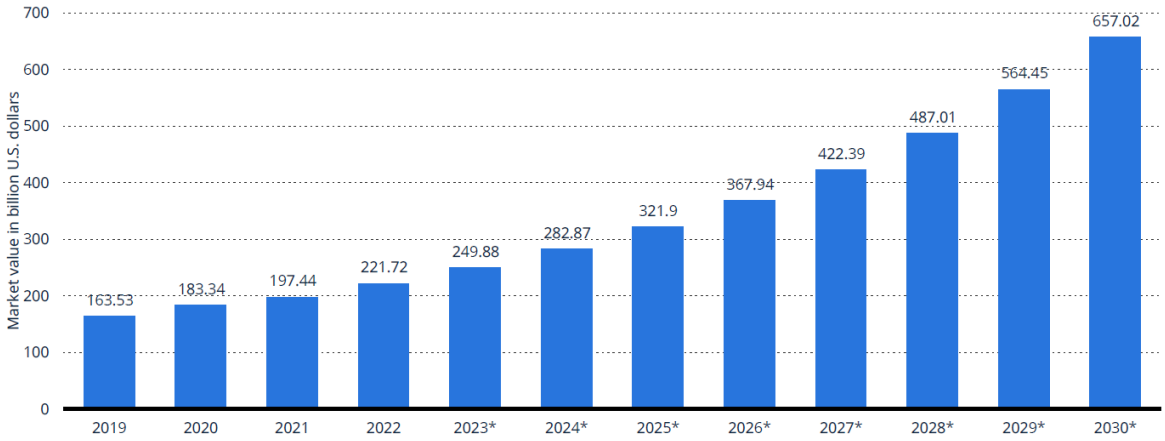

Figura 9. Fatturato del mercato della sicurezza informatica a livello mondiale 2019-2030 [43]

Si osserva dunque una crescita continua del mercato globale della sicurezza informatica. Tale evidenza si manifesta anche nella spesa globale che è cresciuta dal 2017 al 2022, passando da 101,5 miliardi di dollari nel 2017 a 169 miliardi di dollari nel 2022, con una

previsione di crescita nei prossimi anni per cui nel 2024 la spesa mondiale per la sicurezza informatica sarà più che raddoppiata rispetto al 2017 (Figura 10). Gartner ha analizzato come servizi di sicurezza, protezione delle infrastrutture e apparecchiature per la sicurezza delle reti abbiano ricoperto la maggior parte degli sforzi delle organizzazioni [44].

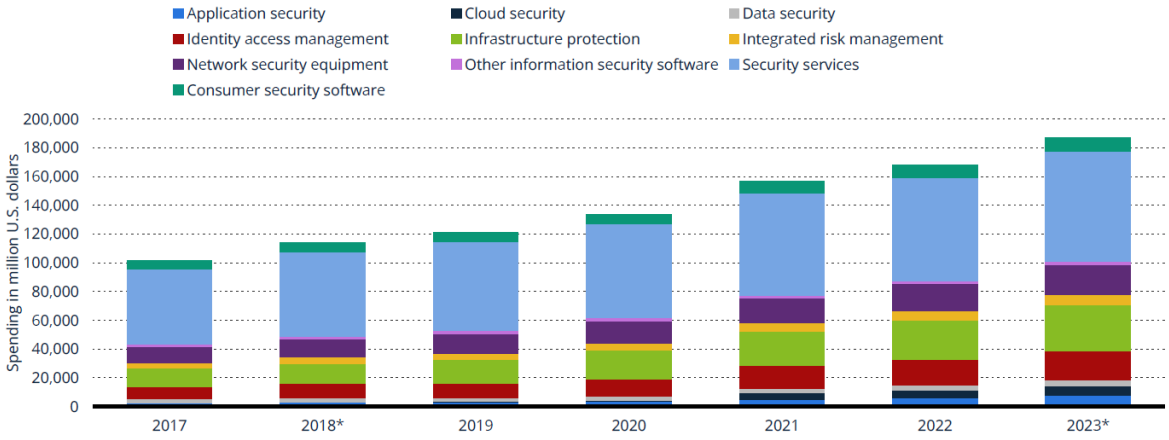

Figura 10. Spesa totale per il mercato globale della sicurezza informatica 2017-2023, per segmento [44]

Dai risultati di una indagine condotta da CompTIA emerge che l'area di cybersecurity più critica nel 2023 sia la sicurezza dei dati, seguita dalla privacy e dalla cybersecurity analytics [45]. La sicurezza dei dati e la sicurezza delle applicazioni sono state nuove opzioni nell'indagine del 2023 e dimostrano chiaramente come le aziende stiano riprogettando le attività di cybersecurity. A parte queste due nuove aree, l'attenzione sembra essere in calo su tutti i temi della cybersecurity. Un'area specifica da tenere d'occhio è l'analisi del rischio, che è il quadro di riferimento per le decisioni in merito agli investimenti e allocazione del budget. Allo stesso modo, l'approccio "zero trust"[5] non è attualmente un approccio definito per molte organizzazioni, ma gli elementi di un'architettura zero trust sono sempre più adottati (Figura 11).

[5] Zero-trust è il nome di un approccio alla sicurezza IT che presuppone l'assenza di un perimetro di rete attendibile e in base al quale ogni transazione di rete deve essere autenticata prima che possa concretizzarsi [46].

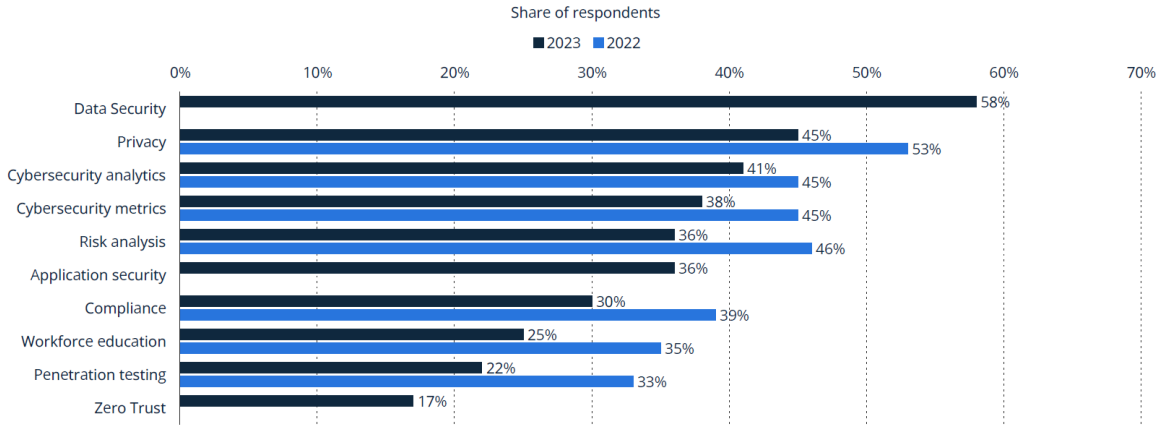

Figura 11. Aree critiche di cybersecurity a livello mondiale 2022-2023 [45]

Con l'aumento della consapevolezza delle minacce informatiche e dell'importanza di avere dei sistemi di sicurezza adeguati da parte delle imprese, il numero di professionisti che lavorano nel settore della cybersecurity è in aumento. Coloro che hanno le competenze necessarie per proteggere sistemi informatici, hardware, rete e dati da attacchi informatici stanno diventando tra le figure più ricercate nel mondo del lavoro odierno, con una domanda che cresce più rapidamente rispetto alla disponibilità. La lotta che i datori di lavoro di tutto il mondo devono affrontare per reclutare professionisti qualificati e competenti per ricoprire ruoli di cybersecurity è in contrasto con i recenti licenziamenti di massa nel settore tecnologico. Sebbene le restrizioni COVID-19, che hanno innescato i licenziamenti nel 2020, si siano allentate nel 2021, fattori come la guerra Russia-Ucraina, l'aumento dell'inflazione e i timori di una recessione economica continuano ad avere un impatto significativo sul settore tecnologico. Nonostante ciò, il numero di professionisti della cybersecurity a livello globale nel 2022 si è attestato a 4,6 milioni, in crescita rispetto ai 4,1 milioni del 2021. La presenza di queste figure ricercate è prevalentemente negli Stati Uniti, in cui il numero è stato stimato in oltre 1,2 milioni nel 2022. Dalla Figura 12 si osserva che l'Italia è indietro rispetto al resto del mondo [47].

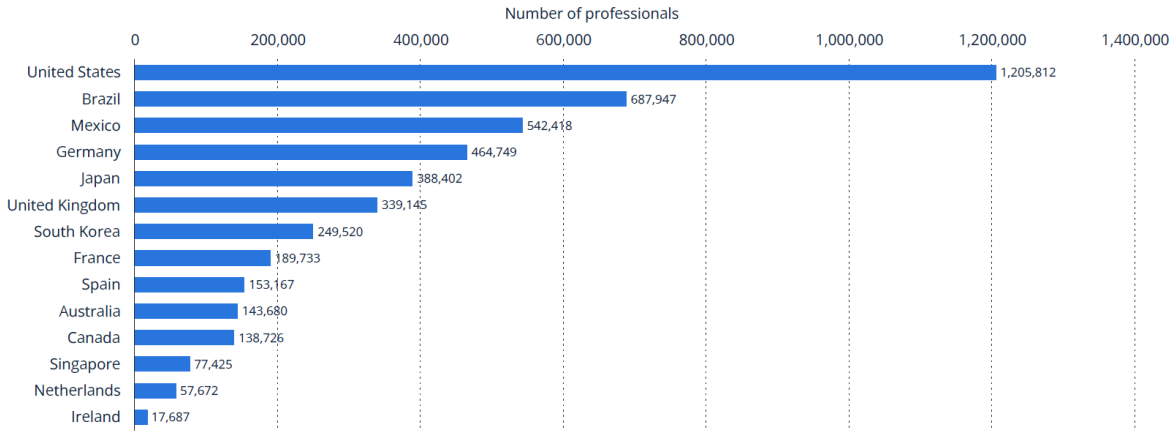

Figura 12. Numero di professionisti della cybersecurity nel mondo nel 2022, per paese [47]

Tra il 2016 e il 2022, la dimensione del mercato del settore della cybersecurity in Italia è cresciuta da 976 milioni di euro a 1,855 milioni di euro, come illustrato in Figura 13 [48].

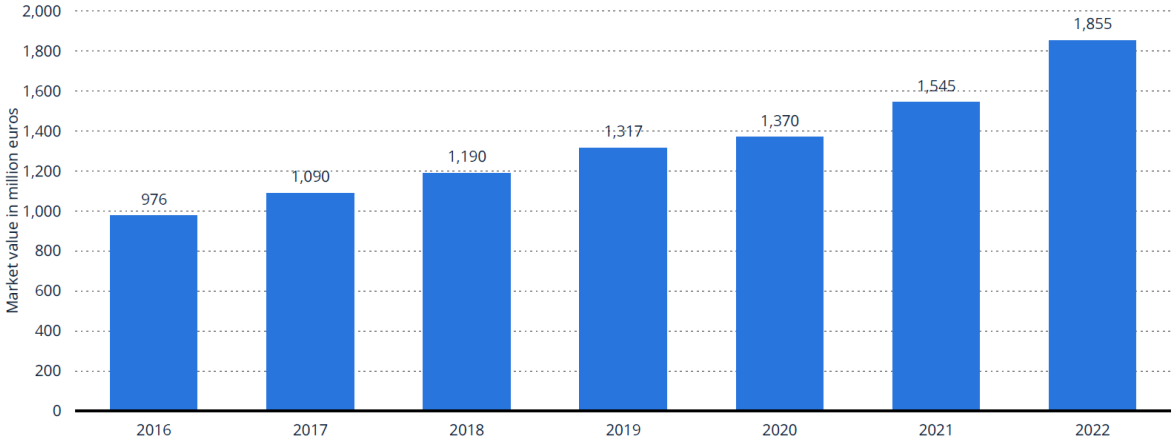

Figura 13. Dimensioni del mercato del settore della cybersecurity in Italia 2016-2021 [48]

In Italia, nel 2022 si è verificato il maggiore incremento percentuale degli ultimi cinque anni negli investimenti in cybersecurity, raggiungendo gli 1,855 milioni di euro investiti e segnando un +18% rispetto al 2021 (Figura 14). Questa è la conseguenza della crescita del numero di attacchi rilevati, discussi nel capitolo precedente [49].

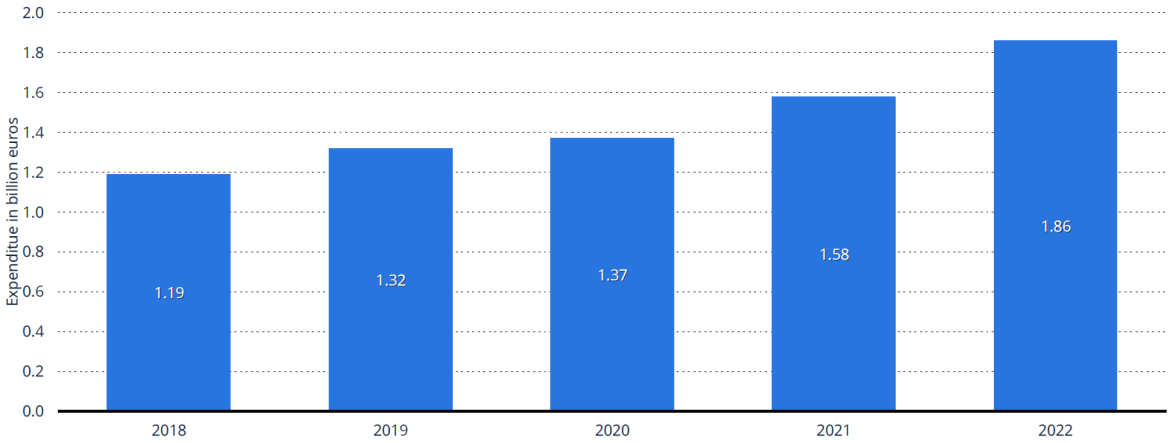

Figura 14. Spesa per il mercato della cybersecurity in Italia 2018-2022 [49]

Ma questo non è sufficiente a posizionare l'Italia in una buona posizione tra le economie avanzate del G7 risultandone anzi l'ultima nel rapporto tra investimenti in cybersecurity e Pil [50]. Ai primi posti spiccano Usa e Regno Unito con lo 0,31% seguono gli altri paesi con una quota tra lo 0,22 e il 0,18% della Germania mentre l'Italia è solo allo 0,1% (Figura 15). Rispetto agli ultimi anni c'è stato un aumento di un paio di decimi di punto.

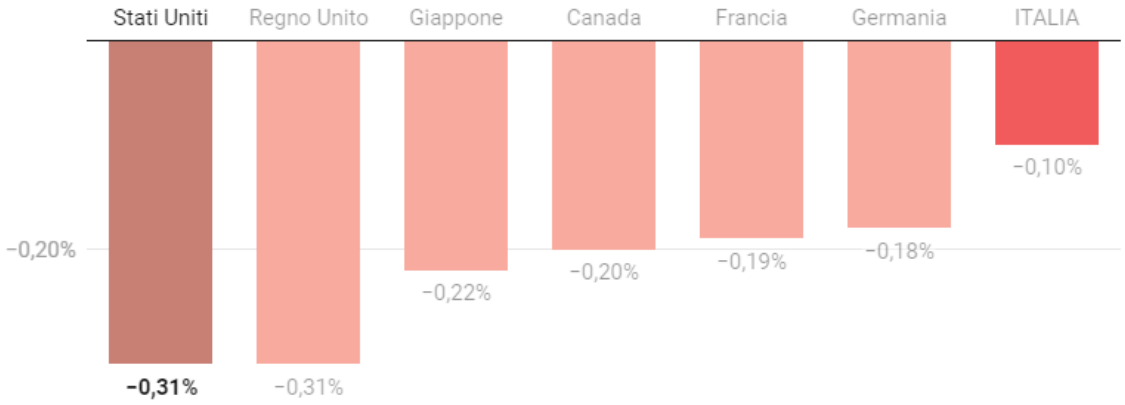

Figura 15. Rapporto tra spesa per la cybersicurezza delle imprese e Pil, nel 2022 (dati in %) [50]

Un dato che fa pensare che il nostro Paese si stia muovendo nella giusta direzione e che stia assumendo consapevolezza dell'importanza della cybersecurity è che in Italia, secondo un sondaggio del 2022, il 61% delle grandi aziende coinvolte ha affermato di aver incrementato il proprio finanziamento per la sicurezza informatica, mentre solo il 3% dei partecipanti ha segnalato una riduzione di tale budget (Figura 16) [51].

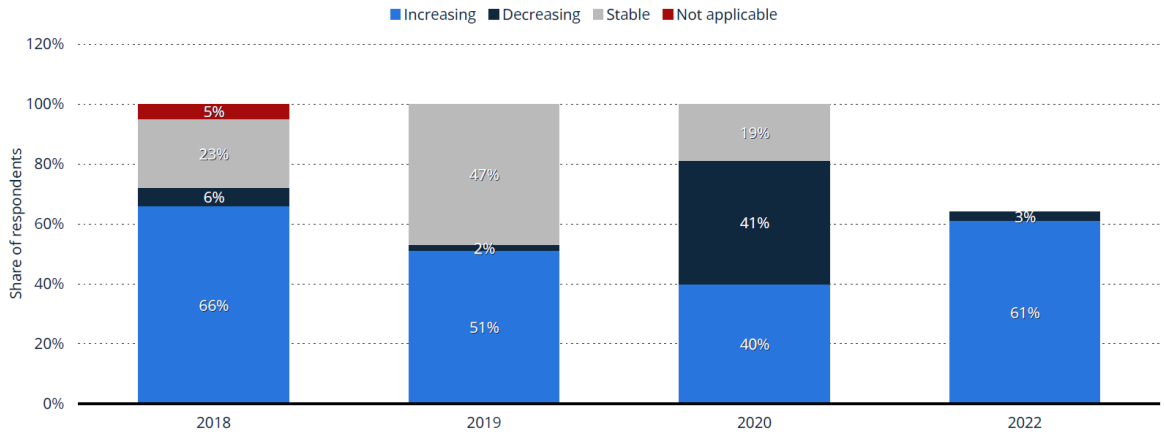

Figura 16. Variazione del budget per la cybersecurity in Italia 2018-2022 [51]

Questa panoramica degli ultimi anni, in cui gli investimenti in cybersecurity hanno raggiunto un livello di importanza senza precedenti, riflette la crescente consapevolezza delle minacce informatiche nel mondo moderno. Con l'aumento esponenziale delle attività online, la protezione dei dati e delle informazioni sensibili è diventata una priorità assoluta per aziende, istituzioni governative e utenti privati. Gli attacchi informatici sempre più sofisticati e mirati richiedono un costante miglioramento delle difese digitali, spingendo le organizzazioni a investire in tecnologie avanzate, formazione del personale e sviluppo di strategie di sicurezza informatica robuste. Questi investimenti non solo proteggono da potenziali danni finanziari e reputazionali, ma sono essenziali per garantire la fiducia del pubblico e mantenere l'integrità delle operazioni aziendali. Inoltre, l'ascesa delle tecnologie emergenti come l'intelligenza artificiale e l'Internet delle cose (IoT – Internet of Things) ha creato nuove sfide e opportunità nel campo della cybersecurity, rendendo gli investimenti continuati e mirati fondamentali per rimanere un passo avanti agli attaccanti digitali. In questo contesto, l'innovazione e l'investimento costante nel campo della sicurezza informatica non solo rappresentano una salvaguardia contro le minacce digitali, ma sono anche un incentivo per lo sviluppo sostenibile e la fiducia nell'ecosistema digitale globale.

1.4 Il ruolo delle policy: iniziative e normative in Italia

In Italia, come in molte altre nazioni, l'importanza delle iniziative, normative e incentivi governativi per la cybersecurity non può essere sottovalutata. Queste svolgono un ruolo cruciale nel garantire la sicurezza delle informazioni sensibili e nel proteggere le organizzazioni e gli individui dalle minacce informatiche sempre più sofisticate e pervasive. Le normative stabiliscono linee guida chiare sulle misure di sicurezza informatica che le aziende devono adottare per proteggere i dati dei clienti e dell'organizzazione stessa. Inoltre, le direttive governative forniscono un quadro normativo che consente alle aziende di

comprendere meglio le proprie responsabilità in termini di sicurezza informatica. Gli incentivi offerti dallo Stato svolgono un ruolo chiave nel promuovere la conformità alle normative di sicurezza cibernetica. Questi incentivi possono assumere varie forme, come agevolazioni fiscali per le aziende che investono in tecnologie e servizi di sicurezza informatica, sussidi per la formazione del personale sulla cybersecurity e finanziamenti per progetti di ricerca e sviluppo nel campo della sicurezza informatica. Questi incentivi non solo stimolano le aziende a investire nella sicurezza cibernetica, ma contribuiscono anche a migliorare la resilienza dell'intera nazione contro le minacce informatiche. Inoltre, le normative e le direttive governative giocano un ruolo essenziale nel garantire la collaborazione tra settore pubblico e privato nella lotta contro le minacce informatiche. Creano un ambiente in cui le aziende sono incoraggiate a condividere informazioni sugli attacchi subiti e sulle nuove minacce scoperte, consentendo alle autorità di adottare misure preventive e investigative in modo più efficace. Quindi, l'adozione e l'applicazione efficace di normative e direttive per la cybersecurity in Italia sono fondamentali per proteggere l'infrastruttura digitale del paese, promuovere l'innovazione tecnologica e garantire la sicurezza delle informazioni per le imprese e i cittadini. Queste misure contribuiscono a creare un ambiente digitale sicuro e affidabile, essenziale per lo sviluppo economico e sociale sostenibile del paese. *"A fronte di un costante aumento degli attacchi nel 2022" ,* segnala Gabriele Faggioli, responsabile scientifico dell'Osservatorio [50], "*molte organizzazioni hanno intrapreso o potenziato gli investimenti in sicurezza adottando nuove tecnologie o rivedendo i processi per proteggersi. È anche merito della spinta propulsiva del Pnrr e sotto la guida della nuova Agenzia per la cybersicurezza nazionale che ha un ruolo fondamentale di indirizzo per un fronte comune per queste sfide. Il mercato della cybersecurity cresce in modo significato e l'aumento degli investimenti pubblici e privati insieme alla chiara strategia istituzionale rappresentano un segnale incoraggiante".*

Il menzionato Piano Nazionale di Ripresa e Resilienza (PNRR) fa parte del programma Next Generation EU (NGEU), un pacchetto da 750 miliardi di euro, metà dei quali rappresentata da sovvenzioni, che è stato approvato dall'Unione Europea in risposta alla crisi pandemica. Il PNRR è strutturato attorno a tre pilastri strategici concordati a livello europeo: la digitalizzazione e l'innovazione, la transizione ecologica e l'inclusione sociale. Questo intervento mira a mitigare gli impatti economici e sociali derivanti dal Covid-19, a indirizzare le vulnerabilità strutturali dell'economia italiana e a guidare il Paese verso una

transizione ecologica e ambientale [52]. Le risorse destinate al Piano Nazionale di Ripresa e Resilienza (PNRR) ammontano a 191,5 miliardi di euro, suddivise in sei missioni:

- Digitalizzazione, innovazione, competitività e cultura - 40,32 miliardi di euro
- Rivoluzione verde e transizione ecologica - 59,47 miliardi di euro
- Infrastrutture per una mobilità sostenibile - 25,40 miliardi di euro
- Istruzione e ricerca - 30,88 miliardi di euro
- Inclusione e coesione - 19,81 miliardi di euro
- Salute - 15,63 miliardi di euro

Per finanziare ulteriori interventi, il governo italiano ha varato un Piano Nazionale Complementare (PNC) con risorse pari a 30,6 miliardi di euro. In totale, gli investimenti previsti dal PNRR e dal Fondo complementare ammontano a 222,1 miliardi di euro [53].
Senza entrare nel dettaglio di ciascuna missione, quella di nostro interesse è quella sulla "Digitalizzazione, innovazione, competitività e cultura" che ha l'obiettivo di favorire l'innovazione in chiave digitale, sostenendo l'infrastrutturazione del Paese e la trasformazione dei processi produttivi delle imprese. Gli investimenti destinati al tema della Cybersecurity, che rientra in questa missione, ammontano a 623 milioni di euro e mirano a potenziare l'ecosistema digitale nazionale attraverso il potenziamento dei servizi di monitoraggio e gestione delle minacce informatiche. Ciò comporterà un significativo potenziamento delle capacità di monitoraggio, prevenzione e risposta ai rischi e agli eventi informatici. Questo sarà possibile grazie a una rete di servizi cibernetici nazionali, adeguatamente integrati con i principali partner sia del settore pubblico che privato [54]. Tale misura si articola in tre pilastri:

- potenziare diffusamente le capacità di cyber resilience[6] nel Paese, promuovendo la collaborazione e l'integrazione tra le capacità di sorveglianza, la condivisione di informazioni e la risposta agli eventi cibernetici;
- potenziare le capacità nazionali di valutazione e certificazione tecnologica per esaminare e certificare beni, sistemi e servizi ICT, attraverso l'istituzione del Centro

[6] Per la definizione di Cyber Resilience si fa riferimento al Cyber Lexicon di FBS (2023*)* [8]: *"The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents."*

di Valutazione e Certificazione Nazionale (CVCN) presso l'ACN (Agenzia per la Cybersicurezza Nazionale);

- potenziare le competenze cibernetiche della Pubblica Amministrazione per garantire la sicurezza dei dati e dei servizi offerti ai cittadini.

Le tappe fondamentali sono riassunte nella Tabella 2.

Tappa	Descrizione	Data prevista	Stato[7]
La nuova Agenzia nazionale	Istituzione e operatività della nuova Agenzia per la Cybersicurezza Nazionale (ACN)	Entro dicembre 2022	Conseguito
Servizi nazionali di cybersecurity	Definizione dell'intero ecosistema della cybersecurity nazionale	Entro dicembre 2022	Conseguito
Avvio della rete di laboratori	Attivazione della rete dei collaboratori di valutazione e certificazione sotto la supervisione del Centro di Valutazione e Certificazione Nazionale (CVCN)	Entro dicembre 2022	Conseguito
Unità centrale ispettiva	Istituzione nell'ambito dell'Agenzia per la Cybersicurezza Nazionale di un'unità interna di audit sulle misure di sicurezza del Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e delle reti e sistemi informativi (NIS)	Entro dicembre 2022	Conseguito
Interventi di potenziamento cyber per la PA	Almeno 5 interventi di potenziamento delle capacità cyber della PA a protezione dei dati e dei servizi dei cittadini	Entro dicembre 2022	Conseguito
Dispiego integrale dei Servizi nazionali di cybersecurity	Attivazione di una rete nazionale integrata di servizi di rilevamento, gestione e mitigazione del rischio cyber a supporto della PA e dell'industria nazionale	Entro dicembre 2024	Da avviare
Rete di laboratori di valutazione e certificazione	Completamento della rete dei laboratori a supporto del conseguimento dell'autonomia strategica nazionale del settore	Entro dicembre 2024	Da avviare

[7] Lo stato è valutato facendo riferimento ad Ottobre 2023 e alle informazioni riportate dal sito: https://www.italiadomani.gov.it/it/Interventi/investimenti/cybersecurity-sicurezza-informatica.html

Servizio ispettivo nazionale	Piena operatività delle attività di monitoraggio tecnico organizzativo dell'adozione delle misure di sicurezza in linea con la normativa di riferimento	Entro dicembre 2024	Da avviare
Interventi di potenziamento cyber per la PA	Almeno 50 interventi di potenziamento delle capacità cyber della PA a protezione dei dati e dei servizi dei cittadini	Entro dicembre 2024	Da avviare

Tabella 2. Tappe fondamentali degli investimenti in Cybersecurity secondo il PNRR

Dunque, gli investimenti si concentrano su quattro principali aree d'intervento [55]:

- potenziamento dei presidi di prima linea per gestire gli avvisi e gli eventi a rischio rivolti alla Pubblica Amministrazione e alle imprese di interesse nazionale;
- creazione o rafforzamento delle competenze tecniche per valutare e sottoporre ad audit continuo la sicurezza di dispositivi elettronici e applicazioni utilizzati per fornire servizi critici da parte di enti che svolgono funzioni essenziali;
- formazione di nuovo personale sia nelle unità di pubblica sicurezza e polizia giudiziaria dedicate alla prevenzione e all'indagine sui crimini informatici diretti contro singoli cittadini, sia in quelle dei settori incaricati di difendere il paese dalle minacce cibernetiche;
- potenziamento degli assetti e delle unità cyber responsabili della protezione della sicurezza nazionale e della risposta alle minacce cibernetiche.

L'ACN, citata precedentemente, è l'Agenzia per la Cybersicurezza Nazionale istituita attraverso il Decreto-legge n.82 del 14 giugno 2021 [56], il quale ha ridefinito la struttura nazionale della cybersicurezza. L'obiettivo principale di questa riforma è stato semplificare il sistema di competenze esistenti a livello nazionale nel campo della sicurezza cibernetica. Questo sforzo è mirato a valorizzare ancora di più gli aspetti di sicurezza e resilienza nel mondo digitale, anche per quanto riguarda la protezione degli interessi nazionali nello spazio cibernetico. L'ACN funge da massima autorità nazionale per la cybersicurezza, incaricata di proteggere gli interessi nazionali nel campo della sicurezza cibernetica. Il suo compito principale è garantire la sicurezza e la resilienza nello spazio digitale. L'Agenzia si impegna attivamente nella prevenzione e mitigazione di attacchi informatici, lavorando anche per promuovere l'autonomia tecnologica del paese. Uno dei compiti chiave dell'ACN è l'attuazione della Strategia Nazionale di Cybersicurezza, approvata dal Presidente del

Consiglio, che stabilisce gli obiettivi da raggiungere entro il 2026 attraverso 82 misure previste [57]. Gli obiettivi di questa strategia sono tre [58]:

- Protezione: la tutela degli asset strategici nazionali avviene mediante un approccio focalizzato sulla gestione e riduzione del rischio. Questo approccio si basa su un quadro normativo e su misure, strumenti e controlli mirati a favorire una transizione digitale resiliente del Paese.
- Risposta: la reazione alle minacce, agli incidenti e alle crisi cyber nazionali avviene attraverso sistemi di monitoraggio, rilevamento, analisi e attivazione di processi che coinvolgono l'intero ecosistema di cybersicurezza nazionale.
- Sviluppo: il progresso sicuro delle tecnologie digitali per soddisfare le esigenze del mercato avviene tramite strumenti e iniziative che supportano i centri di eccellenza, le attività di ricerca e le imprese. Queste azioni sono finalizzate a garantire uno sviluppo sostenibile e sicuro delle tecnologie digitali nel Paese.

Per ognuna delle 82 misure stabilite, suddivise nelle tre aree che mirano a perseguire gli obiettivi sopra descritti, sono definiti gli attori responsabili della loro corretta attuazione attraverso le attività necessarie, le risorse finanziarie a disposizione e rispettando la legislazione vigente comprese le indicazioni del PNRR. La realizzazione della strategia nazionale richiede la collaborazione tra istituzioni, industria e università e appare chiaro come una parte integrante del programma sia la definizione di un ecosistema nazionale di cybersicurezza, in cui sono stabilite le responsabilità di ciascun attore e le modalità del loro coordinamento. Questa idea è alla base del decreto-legge 14 giugno 2021, n.82, che rappresenta la riforma più recente dell'architettura nazionale cyber con cui il legislatore ha deciso di creare un ente centrale che possa essere il riferimento per i diversi attori coinvolti e che possa riordinare le competenze in materia di cybersecurity che prima erano frammentate tra una pluralità di attori istituzionali.

La governance nazionale in materia ad oggi è definita con il quadro rappresentato in Tabella 3:

Attore	**Responsabilità**
Presidente del Consiglio dei ministri	È il vertice dell'architettura istituzionale e organo d'indirizzo politico-strategico in materia. Esercita la direzione ad alto livello e detiene la responsabilità generale delle politiche di cybersicurezza.

Autorità delegata per la sicurezza della Repubblica	Il Presidente del Consiglio può delegare i compiti a questa autorità secondo l'articolo 3 della legge 3 agosto 2007, n. 124.
Comitato Interministeriale per la Cybersicurezza (CIC) Presieduto dal Presidente del Consiglio dei ministri ed è composto dall'Autorità delegata, dal Ministro degli affari esteri e della cooperazione internazionale, dal Ministro dell'interno, dal Ministro della giustizia, dal Ministro della transizione ecologica, dal Ministro dell'università e della ricerca, dal Ministro delegato per l'innovazione tecnologica e transizione digitale, e dal Ministro delle infrastrutture e della mobilità sostenibili.	Istituito presso la Presidenza del Consiglio dei ministri che agisce a livello politico-strategico, con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza. Si occupa di esaminare e indirizzare le problematiche di cybersicurezza, condividere gli obiettivi strategici e monitorare l'attuazione delle politiche in materia. Contribuisce alla realizzazione della strategia nazionale di cybersicurezza ed esercita l'alta sorveglianza sulla sua attuazione.
Agenzia per la Cybersicurezza Nazionale (ACN) che comprende:	Autorità di raccordo con il livello politico-strategico deputata al coordinamento degli attori coinvolti in materia, alla regolamentazione, certificazione e vigilanza del settore. Detiene un ruolo centrale nel raggiungimento nei tre macro-obiettivi della strategia nazionale (visti sopra), nella tutela della sicurezza nazionale e nella salvaguardia degli interessi nazionali.
Computer Security Incident Response Team (CSIRT) Italia	Prevenzione, monitoraggio, rilevamento, analisi, e risposta ad incidenti cibernetici.
Centro di Valutazione e Certificazione Nazionale (CVCN)	Verifica della sicurezza e dell'assenza di vulnerabilità in beni, sistemi e servizi ICT in uso nelle infrastrutture da cui dipendono le funzioni e i servizi essenziali del Paese.
Centro Nazionale di Coordinamento (NCC)	Coordinamento in materia di cybersicurezza nell'ambito industriale, tecnologico e della ricerca.
Altre amministrazioni, tra cui:	
Comparto Intelligence	Conduce attività di ricerca e raccolta informativa in ambito cyber-intelligence finalizzata alla tutela degli interessi politici, militari, economici, scientifici e industriali e provvede alla formulazione di analisi, valutazioni e previsioni sulla minaccia cibernetica.

Ministero dell'interno	Autorità nazionale di pubblica sicurezza. Tra le varie attività svolte, assicura le attività di prevenzione e contrasto ai crimini informatici attraverso la Polizia Postale e delle Comunicazioni.
Ministero della difesa	Autorità per la difesa e la sicurezza militare dello Stato. Definisce e coordina la politica militare, la governance e le capacità militari nell'ambiente cibernetico.
Ciascun Ministero e autorità con competenze e interessi trasversali in materia cyber:	
Ministero degli affari esteri e della cooperazione internazionale (MAECI)	Sviluppa le iniziative di cyber diplomacy, promuovendo la tutela dei diritti e delle libertà nello spazio cibernetico.
Ministero dello sviluppo economico (MISE)	Supporta la transizione digitale dell'industria (PA, PMI) attraverso l'operatività dei Digital Innovation Hub e svolge attività di formazione nella cybersecurity.
Ministero dell'economia e delle finanze (MEF)	Svolge per il tramite della Guardia di Finanza attività di contrasto agli illeciti economico-finanziari commessi per mezzo delle tecnologie informatiche.
Banca d'Italia	Emana regolamenti e linee guida per il rafforzamento della resilienza cyber degli operatori posti sotto la sua supervisione. Riceve le notifiche di incidenti da parte delle banche e degli intermediari finanziari.
Ministero dell'istruzione e Ministero dell'università e della ricerca (MUR)	Promuove un piano strutturato di formazione e di educazione digitale che consenta di colmare la mancanza delle specifiche professionalità richieste dal mercato.
Dipartimento per la Trasformazione Digitale (DTD)	Promuove e coordina le azioni del Governo finalizzate alla definizione di una strategia unitaria in materia di trasformazione digitale della PA e modernizzazione tecnologica del Paese.
Agenzia per l'Italia Digitale (AgID)	Promuove l'innovazione digitale del Paese e l'utilizzo delle tecnologie digitali nell'organizzazione della PA e nel rapporto tra questa, i cittadini e le imprese.
Nucleo per la Cybersicurezza (NCS)	Garantisce l'allineamento tra i diversi attori citati sopra e ha il compito di formulare proposte di iniziativa in materia di cybersicurezza.

Privato: operatori economici, accademia, ricerca, società civile	Collaborano attraverso intese e convenzioni al fine di garantire una proficua interazione con i soggetti che gestiscono asset ICT.

Tabella 3. Governance nazionale in materia di cybersecurity [58]

La definizione della governance sopra riassunta è anche frutto di una continua evoluzione della normativa nazionale in materia di cybersicurezza per fronteggiare l'interconnessione e l'interdipendenza sempre maggiori tra i sistemi informativi e le relative minacce. Negli ultimi cinque anni i provvedimenti in materia di cybersicurezza nel nostro Paese possono essere riassunti come segue:

- **DPCM del 17 febbraio 2017**, che ha rivisto l'organizzazione nazionale per la sicurezza cibernetica già stabilita in precedenza dal DPCM del 23 gennaio 2013 [59].
- **Decreto legislativo 18 maggio 2018, n.65 (decreto NIS)**, che prevede sia l'obbligo di segnalazione degli incidenti che influiscono in modo significativo sulla continuità dei servizi erogati, sia l'obbligo dell'attuazione di misure di sicurezza basate sull'analisi dei rischi per gli Operatori di Servizi Essenziali e i Fornitori di Servizi Digitali [60].
- **Decreto-legge 21 settembre 2019, n.105 (decreto Perimetro)**, che costituisce il Perimetro di sicurezza nazionale cibernetica, con il fine di proteggere gli asset digitali da malfunzionamenti, interruzioni, utilizzo improprio dai quali potrebbe derivare una minaccia per la sicurezza del Paese, stabilendo criteri di notifica degli incidenti e misure di sicurezza più stringenti rispetto a quelle stabilite dal decreto NIS [61].
- **Decreto-legge 16 luglio 2020, n.76**, che provoca la spinta alla digitalizzazione della Pubblica Amministrazione, stabilendo che il processo segua criteri di sicurezza cibernetica, tra cui la formazione dello staff e la promozione della consapevolezza sulla cybersecurity [62].
- **DPCM del 30 luglio 2020, n.131**, che fornisce i criteri per l'individuazione dei soggetti inclusi nel Perimetro Nazionale di Sicurezza Cibernetica [63].
- **Decreto-legge 14 giugno 2021, n.82 (Decreto ACN)**, che apporta disposizioni di cybersicurezza, definisce l'architettura nazionale e istituisce l'Agenzia per la cybersicurezza nazionale (ACN) [56].
- **Strategia Cloud Italia** viene attuata il 18 gennaio 2022, facente parte del Piano triennale per l'informatica nella Pubblica Amministrazione 2020-2022 e definita dal

Dipartimento per la Trasformazione Digitale (DTD) e dall'ACN, e incentiva l'adozione del cloud computing nelle PA [64].

- **Decreto legislativo 8 novembre 2021, n.207**, che è l'attuazione della direttiva 2018/1972 del Parlamento europeo e del Consiglio dell'11 dicembre 2018 e definisce il Codice europeo delle comunicazioni elettroniche e stabilisce i requisiti di cybersicurezza delle reti o dei servizi di comunicazione elettronica pubblici [65].
- **Decreto-legge 21 marzo 2022, n.21**, che ridefinisce gli obblighi e le procedure di notifica delle imprese che fanno uso di servizi basati sulla tecnologia 5G e di altri servizi, beni attività e tecnologie rilevanti per la sicurezza cibernetica, e le procedure di esercizio dei poteri speciali, di monitoraggio e sanzionatori del Governo, affiancando la partecipazione dell'ACN [66].
- **Decreto-legge 18 maggio 2022, n.92 (Decreto Accreditamento cybersicurezza)**, che stabilisce il regolamento che definisce procedure, requisiti e termini per la convalida dei laboratori accreditati di prova (LAP) a sostegno del Centro di Valutazione e Certificazione Nazionale (CVCN) e i raccordi tra CVCN e i Centri di Valutazione del Ministero dell'interno e del Ministero della difesa, al fine di assicurare il coordinamento delle rispettive attività e garantire la massima convergenza [67].
- **DPCM del 15 giugno 2022** [68] e **DPCM del 1° settembre 2022** [69], che trasferiscono in capo all'ACN le funzioni in materia di cybersicurezza precedentemente in capo al Ministero dello sviluppo economico (MISE), all'Agenzia per l'Italia digitale (AgID) e al Dipartimento per la trasformazione digitale.

Abbiamo quindi potuto vedere come il quadro in tema cybersecurity sia delicato, ma è importante considerare anche gli aspetti positivi. In primo luogo, l'ACN svolge un ruolo guida diventando un punto di riferimento per l'intero Paese. Inoltre, l'adozione di una strategia nazionale di cybersicurezza e l'obiettivo di creare un polo strategico nazionale rappresentano significativi progressi nella creazione di un fronte comune contro le minacce informatiche. Da non sottovalutare anche l'aspetto normativo, con l'introduzione continua nel tempo di nuovi provvedimenti. Infine, vista la crescita degli investimenti, c'è una crescente consapevolezza riguardo alla cybersecurity nelle imprese. È evidente allora che negli ultimi anni la sicurezza informatica è diventata uno dei temi principali su cui intervenire e una importante area di investimento, dimostrando che si stanno compiendo sforzi significativi per migliorare e sensibilizzare sul tema della sicurezza informatica.

2. Analisi della letteratura

2.1 Investimento ottimo in sicurezza informatica

Prima di analizzare la letteratura esistente che studia i fattori che determinano gli investimenti in sicurezza informatica in una azienda, che è l'obiettivo del presente lavoro di ricerca, bisogna indagare un aspetto economico fondamentale che tutte le imprese dovrebbero affrontare per una gestione del rischio informatico efficiente, ovvero qual è l'investimento ottimale in attività legate alla cybersicurezza.

Il lavoro di Gordon e Loeb [70] ha ricevuto una notevole attenzione nella letteratura in quanto presenta un modello matematico (modello Gordon-Loeb) per determinare quanto un'azienda dovrebbe investire in sicurezza informatica. In termini matematici, il livello ottimale di investimento è nel punto in cui i costi marginali attesi uguagliano i benefici attesi marginali derivanti da questo. I presupposti di base del modello possono essere riassunti come di seguito:

- La vulnerabilità degli insiemi di informazioni delle organizzazioni è indicata come v $(0 \leq v \leq 1)$ e rappresenta la probabilità di una violazione nelle condizioni di investimento attuali.
- Il valore di un insieme di informazioni, che rappresenta la perdita potenziale in valore monetario, è indicato con L e indica il costo di una violazione.
- La perdita attesa prima di qualsiasi investimento è quindi uguale a vL.
- L'investimento in sicurezza informatica è indicato con z e permette di ridurre la vulnerabilità v. Il prezzo di un'unità di investimento z è uguale a 1.

Il modello Gordon-Loeb definisce la funzione di probabilità di violazione della sicurezza dopo un certo livello di investimenti $S(z, v)$ come differenziabile due volte e strettamente convessa. Le assunzioni che caratterizzano questa funzione sono le seguenti:

- A1. $S(z, 0) = 0$ per ogni z.

Questo vuol dire che un insieme di informazioni non vulnerabile rimane perfettamente protetto per qualsiasi quantità di investimento nella sicurezza delle informazioni, compreso un investimento pari a zero.

- A2. $S(0, v) = v$ per ogni v.

Questo significa che se non ci sono investimenti nella sicurezza delle informazioni, la probabilità di una violazione della sicurezza è la vulnerabilità intrinseca dell'insieme di informazioni.

- A3. Per ogni $v \in (0,1)$ e per ogni z, $\frac{\partial S(z,v)}{\partial z} < 0$ e $\frac{\partial^2 S(z,v)}{\partial^2 z} > 0$ e $\lim_{z\to\infty} S(z,v) = 0$ per ogni v.

Questo comporta che all'aumentare dell'investimento in sicurezza, l'informazione viene resa più sicura, ma a un tasso decrescente. Inoltre, si assume che, investendo sufficientemente in sicurezza, la probabilità di una violazione della sicurezza può essere resa arbitrariamente vicina a zero.

Come si può osservare in Figura 17, i benefici derivanti dall'aumento dell'investimento sono crescenti con un tasso decrescente. I benefici attesi da un investimento in cybersicurezza *EBIS* (*Expected Benefits of an Investment in Information Security)* sono pari alla riduzione della perdita attesa attribuibile alla spesa aggiuntiva:

$$EBIS(z) = [v - S(z,v)]L$$

Se viene sottratto il costo dell'investimento si ricavano i benefici netti attesi di un investimento:

$$ENBIS(z) = [v - S(z,v)]L - z$$

La condizione di primo ordine rispetto a z che massimizza l'equazione di ENBIS è la seguente:

$$-s_z(z^*.v)L = 1$$

Il livello ottimale di investimento in attività legate in cybersecurity z^* si trova nel punto in cui i benefici marginali attesi sono pari al costo marginale atteso.

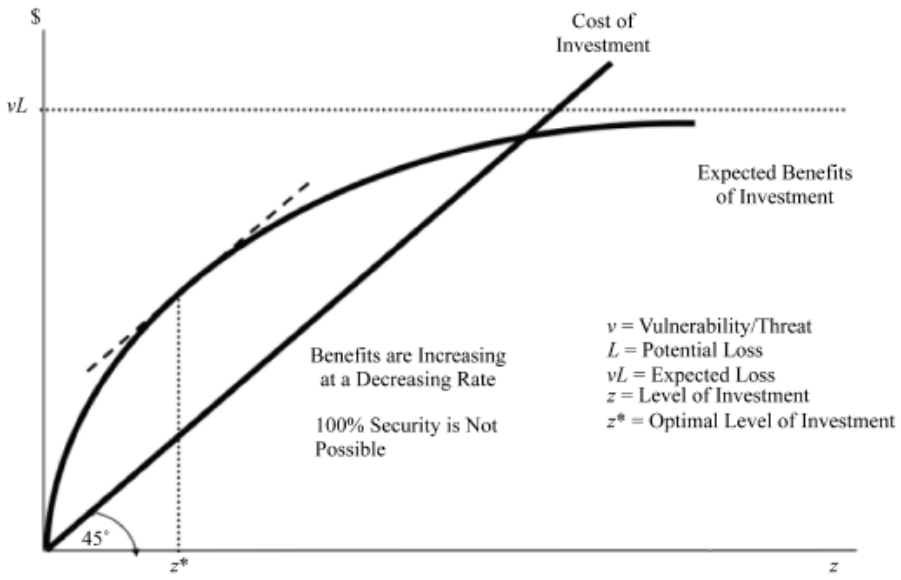

Figura 17. Benefici e costi di un investimento in cybersecurity [70]

Il modello dimostra che questo livello ottimale non supererebbe il 37% (1/e) della perdita prevista derivante da una violazione della sicurezza vL:

$$z^*(v) < \frac{1}{e} * vL$$

In un lavoro successivo, Gordon et al [71] hanno approfondito il modello Gordon-Loeb per l'uso in un contesto pratico come guida per la corretta allocazione delle risorse in attività legate alla sicurezza informatica. Vengono identificate 4 fasi per ricavare l'importo ottimale da investire:

1) Identificazione e valutazione del valore, che corrisponde alla potenziale perdita L, di ciascun set di informazioni nell'organizzazione.
2) Stima della probabilità che un set di informazioni subisca una violazione in base alla sua vulnerabilità v.
3) Creazione di una griglia che raccoglie le possibili combinazioni dei passaggi 1 e 2 e varia da un set di informazioni di basso valore e bassa vulnerabilità a un set di informazioni con alto valore e alta vulnerabilità. All'interno di ogni cella è indicata la perdita attesa vL prima di qualsiasi investimento. Un esempio di griglia è riportato in Figura 18.

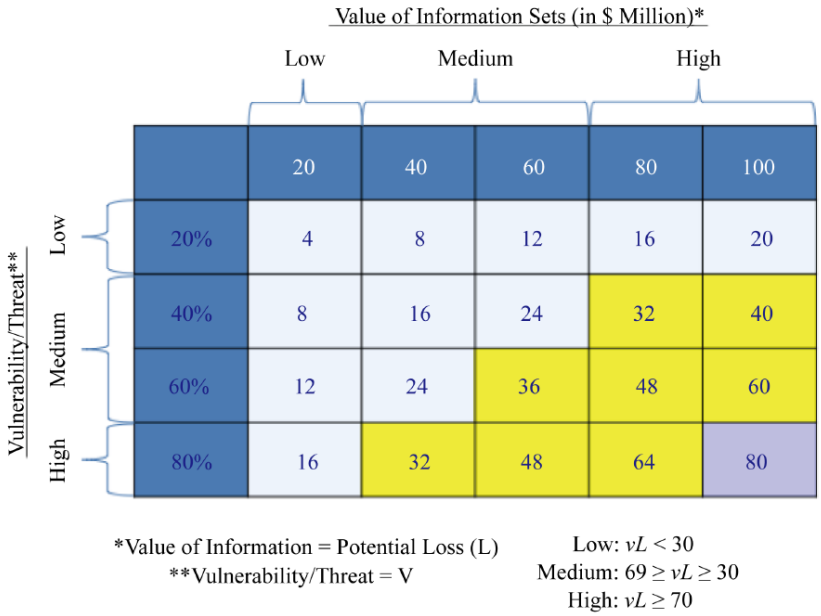

Figura 18. Perdita attesa da una violazione della sicurezza delle informazioni [71]

4) Determinazione del livello di investimento assegnando i fondi per proteggere i diversi set di informazioni. Utilizzando, ad esempio, 1 milione di dollari come unità di investimento in attività di cybersecurity e ipotizzando che gli investimenti siano

generalmente più produttivi laddove le vulnerabilità sono maggiori, è possibile fornire un riepilogo della riduzione della vulnerabilità dovuta agli investimenti incrementali del 1° milione, 2° milione, 3° milione e 4° milione di dollari per ogni livello di v indicato nella Figura 19.

	Low Productivity		Medium Productivity		High Productivity	
z	$s(z,v)$	Reduction in breach Probability	$s(z,v)$	Reduction in breach Probability	$s(z,v)$	Reduction in breach Probability
0	v		v		v	
1	$0.500v$	$0.500v$	$0.250v$	$0.750v$	$0.125v$	$0.875v$
2	$0.333v$	$0.167v$	$0.111v$	$0.139v$	$0.037v$	$0.088v$
3	$0.250v$	$0.083v$	$0.063v$	$0.049v$	$0.016v$	$0.021v$
4	$0.200v$	$0.050v$	$0.040v$	$0.023v$	$0.008v$	$0.008v$
5	$0.167v$	$0.033v$	$0.028v$	$0.012v$	$0.005v$	$0.003v$
6	$0.143v$	$0.024v$	$0.020v$	$0.007v$	$0.003v$	$0.002v$

Low Productivity: $s(z,v)=v/(1+z)$ for Low Vulnerability/Threat
Medium Productivity: $s(z,v)=v/(1+z)^2$ for Medium Vulnerability/Threat
High Productivity: $s(z,v)=v/(1+z)^3$ for High Vulnerability/Threat

Figura 19. Produttività degli investimenti in cybersecurity [71]

Dopo aver valutato i set di informazioni in cui è ancora vantaggioso effettuare l'investimento aggiuntivo di 1 milione di dollari, otteniamo i risultati illustrati nella Figura 20, che mostra gli importi finali da investire in tutti gli insiemi di informazioni. Si può osservare come l'importo massimo da investire in qualsiasi set di informazioni è di 4 milioni di dollari, necessario unicamente ai set di informazioni con un valore di 100 milioni di dollari (L) e un punteggio di vulnerabilità (v) del 20% e del 60% e al set di informazioni con un valore di 80 milioni di dollari e un punteggio di vulnerabilità del 60%.

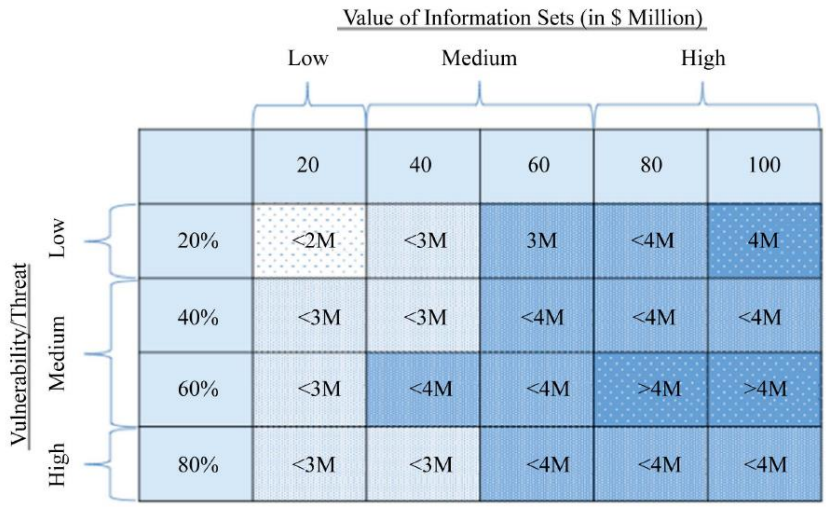

Figura 20. Importi degli investimenti per i set di informazioni [71]

L'utilizzo di questo modello soffre di alcune limitazioni, individuate principalmente nell'imprecisione della valutazione del valore del set di informazioni e della stima della probabilità delle violazioni. Nonostante questi limiti, il modello fornisce un quadro utile per guidare le imprese nella ricerca pratica della corretta spesa in cybersecurity.

Lo studio di Wang e Shaun [72] estende le scoperte di Gordon e Loeb presentando modelli matematici che determinano il limite superiore dell'investimento ottimale, come percentuale del valore a rischio, a seconda di diverse funzioni di probabilità di violazione informatica. A differenza del modello Gordon-Loeb, che considera la probabilità di violazione informatica $v(Z)$ come funzione dell'investimento in sicurezza Z e fissa la vulnerabilità $v(0) = v$ nel caso di investimento in sicurezza zero ($Z = 0$), Wang e Shaun ancorano la funzione di probabilità di violazione informatica ad un investimento $B > 0$, chiamato *benchmark spending,* considerando che tipicamente le aziende hanno già investito in qualche misura protettiva. Allora, qualsiasi importo di spesa per la sicurezza Z può essere descritto dal rapporto di spesa, $z=Z/B$ e si denota la probabilità di violazione informatica con $v(z)$. Con una spesa di riferimento B, abbiamo $z = 1$ e $v(1)$. La funzione di probabilità della sicurezza $v(z)$ è caratterizzata dalle seguenti condizioni:

- $v(0)=1$. Quando la spesa per la sicurezza è pari a zero, c'è probabilità 1 di essere violati.
- $v'(z) < 0$, per z>0. All'aumentare dell'investimento in sicurezza z, la probabilità di violazione informatica $v(z)$ diminuisce.
- $v'(z)$ è funzione continua di z.

Il costo informatico è dato dalla somma della spesa per la sicurezza Z e delle perdite annuali previste, individuate di seguito nei due termini rispettivamente:

$$Cost(z) = z * B + v(z) * R$$

Le perdite annuali previste sono date dal prodotto di R, che è il valore a rischio in caso di violazione, e $v(z)$, che è la probabilità di attacco informatico.

Il rapporto di spesa ottimale z^* è definito in modo tale che il costo informatico dell'azienda sia ridotto al minimo alla spesa per la sicurezza $Z^*=z^*\cdot B$. Uguagliando la derivata di $Cost(z)$ rispetto a z a zero, si ottiene:

$$\frac{dCost(z^*)}{dz} = B + v'(z^*) * R = 0$$

Il livello ottimale di spesa per la sicurezza $Z^*=z^*\cdot B$ soddisfa l'equazione:

$$-v'(z^*) = B/R$$

Il derivato $-v'(1)$ indica l'efficacia della spesa incrementale nel ridurre la vulnerabilità, in corrispondenza del benchmark di spesa B.

Esaminando le seguenti classi di funzione di probabilità di violazione informatica si verifica che hanno tutte la proprietà di invarianza, con la forma funzionale e il parametro α che rimangono invariati per diverse scelte del benchmark B e si dimostra che l'investimento ottimale in sicurezza $Z^*=z^*\cdot B$ ha come limiti superiori:

1) Classe di potenza esponenziale: $v_{EP}(z) = v(1)^{z^\alpha},\ Z^* \leq \frac{\alpha}{e} * R$
2) Classe di rischio proporzionale: $v_{PH}(z) = 1 - [1 - v(1)]^{z^{-\alpha}},\ Z^* \leq \frac{\alpha}{e} * R$
3) Classe di trasformazione di Wang: $v_{WT}(z) = \Phi[\Phi^{-1}(v(1)) - \alpha * ln(z)],\ Z^* \leq \frac{\alpha}{\sqrt{2\pi}} * R$

Lo studio, quindi, fornisce la prova che la regola 1/e per l'investimento in sicurezza ottimale in Gordon-Loeb vale per le classi di potenza esponenziale e di rischio proporzionale. Tuttavia, per la classe di trasformazione Wang, abbiamo la regola $1/\sqrt{2\pi}$ (superiore a 1/e). Pertanto, il limite superiore dell'investimento ottimale in sicurezza dipende dalla forma funzionale specifica della probabilità di violazione informatica.

Questa conclusione è confermata anche da Hausken [73] che indaga l'effetto di diverse ipotesi di rendimento sul livello ottimale di investimento e sulla sensibilità alle variazioni del livello di vulnerabilità. Il suo studio mostra come l'investimento ottimale non è più limitato al 37% $(1/e)$ della perdita attesa e analizza quattro tipi di rendimenti marginali: decrescente, prima crescente e poi decrescente (funzione logistica), crescente e costante.

Gordon e Loeb considerano rendimenti marginali decrescenti caratterizzanti due classi di funzioni di probabilità soddisfano le tre ipotesi A1, A1, A3 viste nel modello Gordon-Loeb: $S^I(z,v) = v/(\alpha z + 1)^\beta$ e $S^{II}(z,v) = v^{\alpha z+1}$. Partendo da queste, si possono fare confronti con altre funzioni con rendimenti marginali differenti. Ad esempio, in alternativa alla decrescita convessa di $S(z,v)$ in A3 consideriamo la decrescenza logistica specificata dall'assunzione A4: per tutti i $v \in (0,1)$, e tutti gli z, $\frac{\partial S(z,v)}{\partial z} < 0$ e $\frac{\partial^2 S(z,v)}{\partial^2 z} < 0$ per $0 \leq z \leq z_i$, e $\frac{\partial^2 S(z,v)}{\partial^2 z} > 0$ per $z \geq z_i$, dove z_i è un investimento intermedio tale che $\frac{\partial^2 S(z,v)}{\partial^2 z} = 0$ e $\lim_{z\to\infty} S(z,v) = 0$ per tutti i v. In questo caso, l'impatto dell'investimento aumenta dapprima in modo crescente e poi in modo decrescente. La funzione logistica decrescente, che chiamiamo classe III, può essere formulata come $S^{III}(z,v) = \frac{v}{1+\gamma(e^{\emptyset z}-1)}$.

Se la funzione di probabilità di violazione della sicurezza $S(z,v)$ è di classe III, cioè logisticamente decrescente e soddisfa i seguenti criteri A1, A2, A4, allora l'investimento ottimale come frazione della perdita attesa da una violazione della sicurezza non soddisfa $z^{III*}(v)/vL < 1/e$. Infine, per i rendimenti marginali crescenti e rendimenti marginali di scala costanti della sicurezza dell'informazione, il livello ottimale di investimento è zero per i bassi livelli di vulnerabilità, e salta al massimo per i livelli intermedi. Per le vulnerabilità più elevate è costante in termini assoluti, e diminuisce in modo convesso in termini di perdita attesa. Naturalmente, è una questione empirica stabilire quale di queste classi di violazioni della sicurezza catturi meglio il fenomeno del mondo reale.

Tra gli altri paper in cui si vuole determinare la percentuale del limite superiore dell'investimento ottimo, Willemson [74] esamina l'utilizzo di funzioni di probabilità lineari per esplorare situazioni in cui i ritorni marginali rimangono costanti. In questa specifica condizione, è possibile neutralizzare completamente i cyberattacchi investendo una quantità sufficiente di risorse. Questo porta alla conclusione che il limite massimo dell'investimento ottimale tende verso il 100%.

Analizzando funzioni di probabilità generiche, Baryshnikov [75] e Lelarge [76], che generalizzano Gordon e Loeb, identificando una proprietà matematica che deve essere soddisfatta affinché l'investimento ottimale sia limitato superiormente. Concludono che se la funzione di probabilità è decrescente e presenta una convessità logaritmica rispetto all'ammontare dell'investimento, l'investimento ottimale è vincolato al 36,8% della perdita attesa senza alcuna protezione.

Gli studi citati fino ad ora analizzano il quadro di riferimento che non considera interdipendenza tra le imprese e si basa su un modello a un periodo con un solo decisore.
Dopo aver analizzato gli studi che hanno condotto a modelli matematici per trovare l'investimento ottimo, bisogna valutare i modi in cui le organizzazioni prendono le decisioni in merito alla spesa per la sicurezza informatica.
Vista la natura incerta, in termini di probabilità di accadimento, delle violazioni della sicurezza potrebbe essere non conveniente dal punto di vista del rapporto costi-benefici cercare di prevenirle tutte perché potrebbe comportare un sovrainvestimento. Può invece convenire avere un atteggiamento "wait and see" investendo inizialmente una parte del budget e rimandare il resto fino a quando non si verificano effettivamente le violazioni. A tal proposito, Gordon et al. [77] hanno applicato l'approccio delle opzioni reali ad un caso pratico per dimostrare il beneficio di aspettare che si verifichino le violazioni prima di investire piuttosto che agire preventivamente. La teoria mostra che investire oggi è più conveniente se il valore attuale netto dell'investimento odierno è maggiore del valore di opzione associato alla decisione rinviata. Nella Figura 21 viene rappresentato l'esempio pratico studiato con il quale si valuta il valore dell'opzione di investire quando si hanno informazioni sulla violazione rispetto all'investire adesso. Per semplicità, si considera un'impresa che ha 1 milione di dollari da investire in operazioni di cybersicurezza e che i costi associati alle violazioni, prima dell'investimento, ammontino in media a 40.000 o 200.000 dollari a seconda dell'efficacia del sistema di sicurezza attuale. L'investimento coprirebbe un anno di attività e permetterebbe di evitare le presunte minacce generando un potenziale risparmio di 480.000 dollari (ovvero 12 x 40.000 dollari) o di 2.400.000 dollari (12 x 200.000 dollari). Ipotizzando che i risultati siano ugualmente probabili, il valore netto atteso dell'investimento sarebbe di 440.000 dollari (ovvero 0,5 x 480.000 dollari + 0,5 x 2.400.000 dollari). Successivamente, viene ipotizzato che gli attacchi si rivelino dopo un mese e che l'investimento di 1 milione di dollari possa essere rimandato di un mese con copertura per gli 11 mesi restanti. Dopo il primo mese l'impresa ha l'informazione se i risparmi sui costi sono di 440.000 dollari (ovvero 11 x 40.000 dollari) o di 2.200.000 dollari (ovvero 11 x 200.000 dollari). Nel primo scenario non conviene investire perché i benefici non sono sufficienti a giustificare l'investimento. Al contrario, nel secondo scenario i benefici sono superiori dell'investimento ma la probabilità che si verifichino è del 50% portando ad un valore netto atteso di 600.000 dollari (ovvero 0,5 x 1.200.000 dollari). Si osserva che il valore dell'opzione di rinviare la spesa in cybersecurity è di 160.000 dollari

(ovvero 600.000 dollari – 440.000 dollari) e conviene rimandare la decisione di investire. Questo esempio dimostra come l'incertezza associata alle violazioni cyber possa giustificare un approccio attendista "wait and see" prima di destinare tutti i fondi nelle difese informatiche.

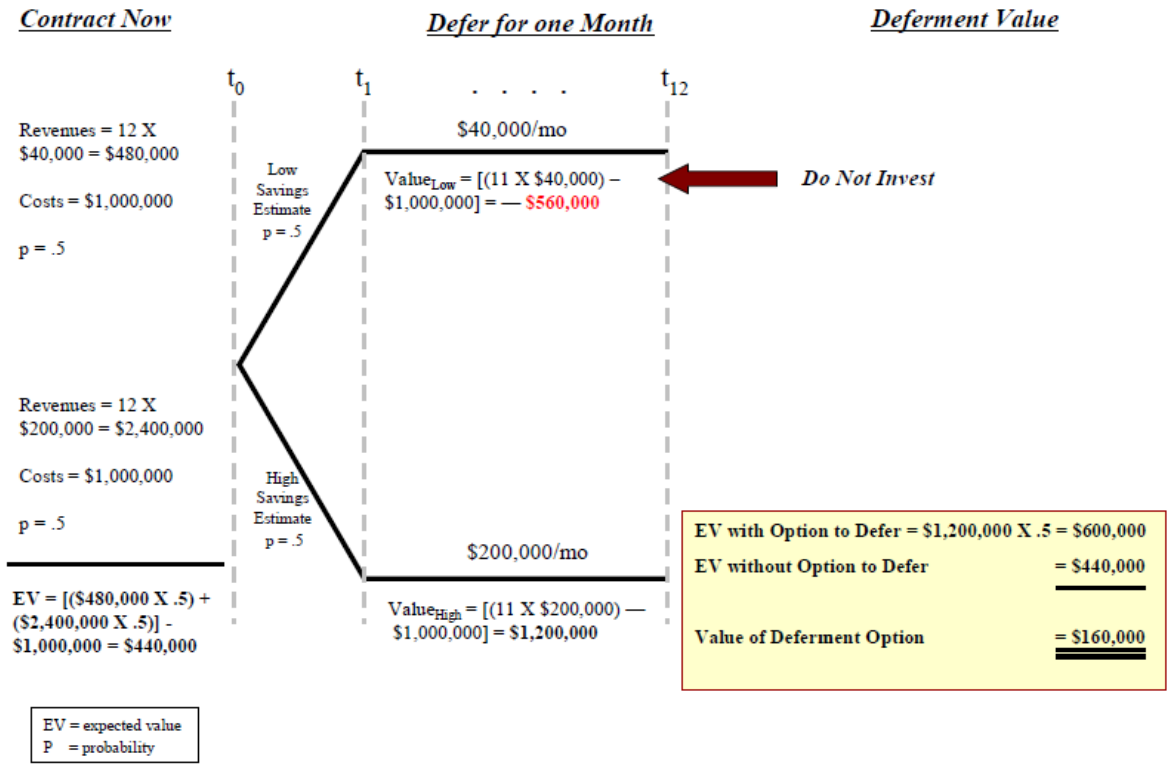

Figura 21. Esempio pratico di valore dell'opzione di rinviare l'investimento in cybersecurity [77]

A sostegno dell'ipotesi che le effettive minacce incidano sulla scelta delle imprese di investire Gordon et al. hanno effettuato un'indagine in cui è stato chiesto ai dirigenti il livello di disaccordo o accordo sul fatto che una vera e propria violazione fosse un fattore determinante delle spese in sicurezza informatica. La risposta è stata misurata su una scala da 1 a 7 (1 indica un forte disaccordo e 7 un forte accordo) e la maggior parte degli intervistati ha indicato che un attacco è un fattore importante nella decisione di investire (21 dei 38 intervistati hanno segnato un 5, 6 o 7 sul livello di accordo). I risultati supportano l'evidenza che molte aziende aumentano le spese per la sicurezza delle informazioni in seguito a una violazione. Questo approccio reattivo, anziché proattivo, è coerente con la visione delle opzioni reali degli investimenti di capitale vista in precedenza.

Anche Krutilla et al. [78] estendono il modello di Gordon e Loeb a un periodo più lungo, affrontando una decisione di investimento aziendale su un orizzonte temporale infinitamente lungo. In questo contesto, gli asset di cybersecurity, come software, hardware e risorse umane specializzate nella sicurezza, subiscono ammortamento nel tempo e i benefici netti

dell'investimento sono attualizzati. Gli autori dimostrano che l'investimento ottimale nella cybersecurity è negativamente influenzato dalla combinazione del tasso di ammortamento e del tasso di sconto. Dal momento che prove empiriche indicano che questa combinazione è di solito inferiore a uno, a differenza del modello statico di Gordon e Loeb in cui è uguale a uno per definizione, Krutilla et al. concludono che un'analisi a un solo periodo potrebbe sottostimare l'entità ottimale dell'investimento necessario.

Un approfondimento sulla distinzione tra approccio reattivo e proattivo è stato fatto da Rowe e Gallaher [79]. Sulla base di interviste sottoposte a organizzazioni private degli Stati Uniti di diversi settori industriali hanno osservato che le imprese manifatturiere sono le più proattive, seguite da quelle sanitarie e finanziarie. La componente di costo maggiore dell'adozione di strategie proattive è legata alla valutazione e al test di nuove procedure di sicurezza informatica. Viene provata una correlazione tra la strategia di sicurezza e la sua dipendenza dalle informazioni pubbliche esterne al processo decisionale per cui le industrie che hanno maggiori informazioni perseguono strategie più proattive. Il diagramma di flusso del processo decisionale schematizzato da Rowe e Gallaher prevede due fasi principali:

- Determinazione di una strategia di investimento in cui il management dà priorità alle esigenze di sicurezza informatica previste o fissa un budget. Nel primo caso il management identifica le necessità di sicurezza e stabilisce, di conseguenza, il livello di investimento, mentre nel secondo determina il livello di spesa da stanziare in sicurezza informatica e gli acquisti sono fatti massimizzando l'utilità delle risorse.
- Implementazione della strategia in cui il personale IT determina l'approccio più efficiente per soddisfare le esigenze di sicurezza dell'organizzazione valutando le informazioni ottenute da fonti esterne e interne, che sono riassunte in Figura 22.

Internal	External Public	External Private
	DRIVERS	
Business Process needs (i.e., strong business reliance on network) Major past breach	Regulations	Client demands Supplier demands
	INFORMATION RESOURCES	
Internal audits Staff experience/training Internally collected/calculated data (e.g., number of compromises, cost estimates) CEO/CTO/COO/etc. suggestions	NIST best practices ISO guidelines American National Standards Institute (ANSI) guidelines Security impact estimated (e.g., CSI/FBI survey) CERTS, SANS, etc.	Customer suggestions/ requirements Vendor suggestions/advice Conferences or trade publications Outside consultants Other organizations External audits

Figura 22. Categorizzazione dei drivers rilevanti e delle risorse di informazioni [79]

Il compromesso tra l'implementazione di una strategia reattiva (R) e una strategia proattiva (P) è determinato prendendo spunto dalla teoria microeconomica ed è rappresentato nel grafico in Figura 23. Le curve concave rispetto all'origine sono le cosiddette curve di iso-sicurezza, per cui all'allontanarsi dall'incrocio degli assi aumenta il livello di sicurezza. La linea retta, invece, indica il vincolo di budget in dollari: se l'organizzazione destinasse tutte le risorse per la sicurezza informatica a una strategia proattiva, si troverebbe nel punto contrassegnato da $\$/P_A$; in alternativa, se destinasse tutte le risorse per la sicurezza informatica a una strategia reattiva, si troverebbe nel punto contrassegnato da $\$/P_R$, dove P_A e P_R sono concettualmente il prezzo unitario di un'attività proattiva e reattiva, rispettivamente. Seguendo l'approccio di massimizzazione del livello di sicurezza considerando il vincolo di bilancio, il mix di strategie reattive (R) e proattive (A) ottimo si trova nel punto di tangenza tra la linea del budget e la curva di iso-sicurezza più alta che può essere raggiunta. Se, invece, si vuole seguire l'approccio di minimizzazione dei costi considerando un livello di sicurezza fisso, la linea di budget viene regolata in base al livello totale di spesa necessario per raggiungere la sicurezza desiderata e alla percezione del costo di essere più proattivi o più reattivi. Quindi, la combinazione di equilibrio si basa sul livello di sicurezza stabilito e sulla linea di budget che crea un punto di tangenza. In questo modo, l'azienda può spendere il livello ottimale di investimenti in strategie proattive e reattive in base a uno specifico livello di sicurezza desiderato.

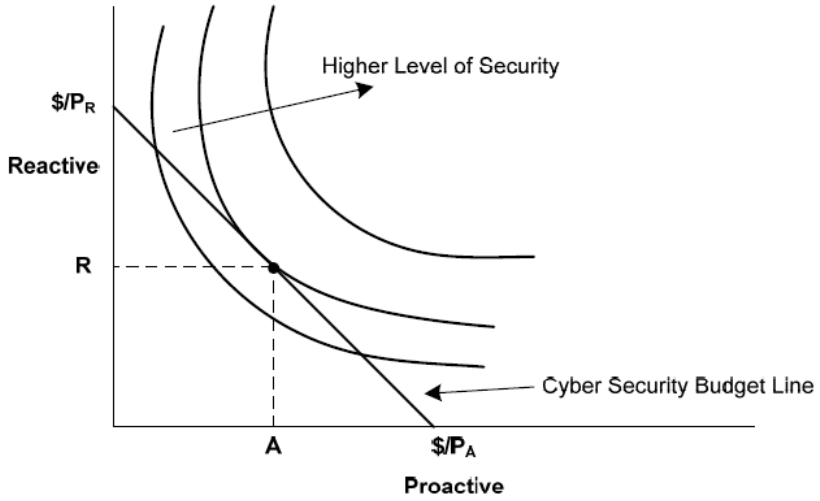

Figura 23. Equilibrio tra strategie reattive e proattive [79]

Un ulteriore studio che fornisce una visione del processo decisionale utilizzato dalle organizzazioni per gli investimenti in cybersecurity è quello di Kisson e Tara [80], in cui, attraverso l'uso di una indagine pubblicata tra il 2018 e il 2019 che ha raccolto un totale di

100 partecipanti, sono emersi i seguenti risultati divisi in tre categorie. La prima valuta l'efficacia delle attuali implementazioni dei framework di cybersecurity: 93 intervistati hanno dichiarato che utilizzano i framework governativi e di settore per implementare le misure di sicurezza e 84 hanno indicato che hanno basato le loro decisioni per essere conformi alle normative, standard di settore e policy interne. Inoltre, 89 intervistati hanno indicato che le priorità in base a cui si misura l'efficacia del framework di cybersecurity sono le seguenti:

- conformità
- test di audit/assicurazione
- indicatori chiave di performance
- modelli di maturità delle capacità
- costo

La seconda categoria indaga i fattori utilizzati da un'organizzazione nella valutazione e nell'implementazione delle misure di sicurezza quando investe in cybersecurity e 87 intervistati hanno indicato i seguenti:

- conformità alle normative governative e di settore
- costo dell'investimento
- impatto di una violazione o di una multa
- rischio di reputazione o di marchio
- facilità di utilizzo da parte dell'azienda

Infine, la terza categoria, si concentra sull'importanza degli stakeholders nel processo decisionale utilizzato all'interno dell'organizzazione per valutare, implementare e investire nei controlli di cybersecurity e 89 intervistati hanno indicato la seguente gerarchia di decisori:

- Chief Technology Officer (CTO)
- Chief Information Security Officer (CISO)
- Responsabile della linea di business
- Chief Information Officer (CIO)
- Consiglio di amministrazione

Abbiamo visto che l'allocazione del budget in misure di sicurezza informatica è un'attività critica nel processo decisionale di un'impresa. Nonostante le organizzazioni abbiano attivamente implementato misure di sicurezza e il 75% degli intervistati dichiara di essere in grado di rilevare, rispondere e monitorare un incidente cyber, il 54% del campione ha

segnalato di aver subito una violazione della cybersicurezza e il 94% ha espresso una perdita media compresa tra 0 e 1 milione di dollari. Inoltre, la prevenzione degli attacchi è maggiormente complessa da raggiungere perché il 93% dei partecipanti ritiene che il budget per la cybersecurity della propria organizzazione sia insufficiente per garantire misure di cybersecurity adeguate a prevenire una violazione. Questo dimostra come sia necessario migliorare il processo decisionale per ridurre il numero di violazioni e facilitare un processo preventivo.

Parte di questi risultati sono confermati da Moore et al. [81] che provano, dopo aver intervistato 40 dirigenti di grandi aziende di quattro settori (sanità, finanza, commercio al dettaglio e pubblica amministrazione), come i primi possibili fattori che spingono gli investimenti in sicurezza sono la riduzione del rischio percepito e le conformità alle norme e agli standard di settore, come si può vedere in Figura 24.

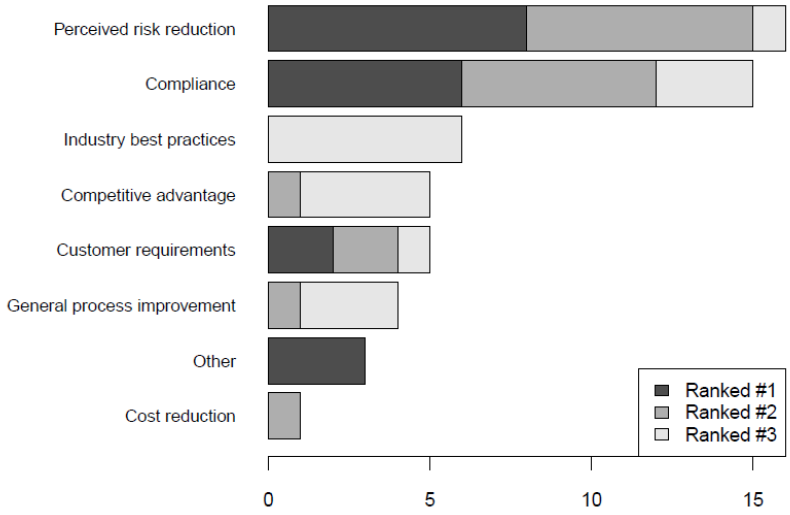

Figura 24. Classifica dei drivers degli investimenti in sicurezza delle informazioni [81]

Successivamente, hanno individuato gli approcci più utilizzati in elenco di priorità e le prime due scelte sono state le best practice di settore e i framework. La maggior parte dei direttori della cybersecurity intervistati utilizza un framework per definire lo stato di cybersecurity della propria sicurezza e per dare priorità agli investimenti. Questi framework variano da

quelli più noti come l'ISO[8] e il NIST[9], fino a framework di tipo "homegrown" che possono essere una combinazione di framework esistenti o completamente personalizzati. L'utilizzo di un framework ha avuto una leggera correlazione con la concezione di spendere abbastanza o troppo poco: tutte le aziende che ritenevano di spendere in modo adeguato avevano un quadro di riferimento. Gli "attacchi passati alla vostra azienda" si sono piazzati al terzo posto, con un risultato sostanziale ma minore per gli "attacchi passati ad altre aziende". I risultati sono riportati in Figura 25.

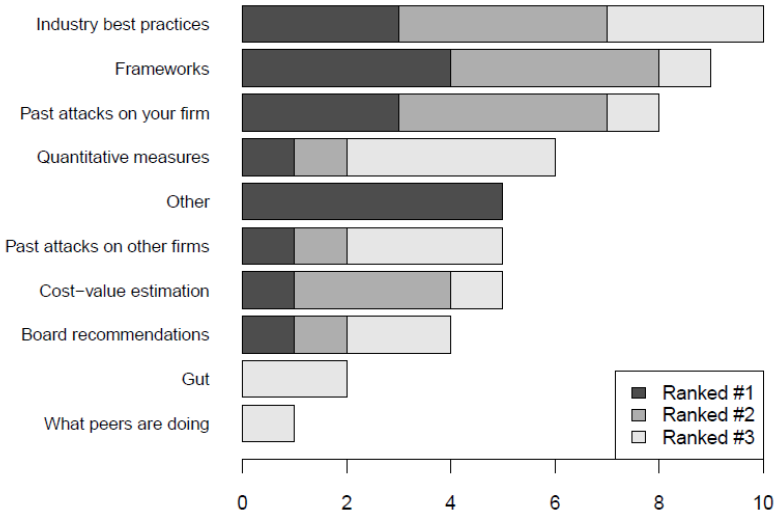

Figura 25. Prioritizzazione degli approcci alla sicurezza informatica [81]

Una prova degna di essere considerata ottenuta dal loro studio è, inoltre, quella per cui il management delle imprese ha compreso l'importanza di investire in cybersecurity. Infatti, l'81% dei soggetti ha dichiarato che il management di alto livello è di supporto alle loro attività e l'85% ha riferito che il livello di supporto è in aumento, mentre il resto ha dichiarato che il supporto è rimasto invariato. Nessuno ha affermato che il supporto ricevuto in materia di cybersecurity è diminuito. In aggiunta, al di fuori della pubblica amministrazione, i budget per la cybersecurity sono generalmente in crescita. L'88% dei partecipanti riferisce che il budget per la sicurezza è aumentato, mentre il resto dichiara che è rimasto invariato.

---

[8] Sviluppato dall'International Standards Organization (ISO), lo standard ISO 27001 fornisce alle organizzazioni i requisiti su come gestire e proteggere le loro informazioni aziendali sensibili con un cosiddetto Information Security Management System (ISMS).

[9] Il NIST (National Institute of Standards and Technology) è un'agenzia non regolatoria che promuove l'innovazione attraverso il progresso della scienza, degli standard e della tecnologia delle misurazioni. Il NIST CSF (NIST Cybersecurity Framework) consiste in standard, linee guida e best practice per aiutare le organizzazioni a migliorare la logo gestione dei rischi per la sicurezza informatica.

2.2 Effetti delle esternalità di rete sull'investimento ottimo in sicurezza informatica

Abbiamo compreso come la mancanza di analisi quantitative per valutare la questione degli investimenti in sicurezza informatica sia una barriera per le imprese, ma almeno altre due limitano la capacità di un'organizzazione di determinare la propria strategia ottimale di investimento in sicurezza informatica. La prima barriera è la limitata disponibilità di informazioni affidabili che sarebbero necessarie per prendere decisioni di investimento informate. Il secondo ostacolo è rappresentato dalle esternalità e dalla natura di bene pubblico della conoscenza della sicurezza informatica.

In merito alle esternalità generate dalla interdipendenza tra le imprese, Fedele e Roner [82] identificano spillovers tecnici e spillovers di mercato. I primi si manifestano quando le organizzazioni sono connesse da una rete informativa comune ma non sono concorrenti sul mercato, mentre i secondi quando le imprese sono concorrenti ma usano sistemi informatici non comuni.

L'effetto di uno spillover tecnico è quello di ridurre la probabilità di subire una violazione della sicurezza da parte di tutte le imprese all'interno della rete di quella che fa l'investimento. Questo comporta che, all'aumentare delle ricadute positive degli spillovers tecnici, l'investimento di equilibrio ottimo è sempre più basso. È evidente un problema di free-riding per cui, al crescere del numero di imprese all'interno della rete, ognuna di queste può godere delle esternalità positive e al limite, cioè quando la numerosità tende ad infinito, l'investimento si avvicina a zero perché nessuna impresa è disposta ad investire. Inoltre, quando un'impresa decide di aumentare l'investimento in sicurezza informatica, il beneficio marginale privato è inferiore al beneficio marginale sociale perché il primo non interiorizza la riduzione della probabilità di subire una violazione di cui godono le altre imprese. Il risultato è che le organizzazioni investono troppo poco in cybersecurity.

Nel caso di spillovers di mercato, l'investimento in cybersecurity di un'impresa non influisce sul livello di protezione dei concorrenti. L'effetto delle ricadute di mercato può essere modellato in modo che l'impresa che subisce un cyberattacco perde la sua quota di ricavi che viene suddivisa tra le altre che non sono state colpite e fanno parte dello stesso mercato. Il risultato prodotto è il medesimo delle ricadute tecniche ma per un meccanismo diverso dal free-riding. L'investimento di equilibrio diminuisce quando si passa da monopolio a duopolio perché l'impresa monopolistica che investe ha maggiori probabilità di non subire violazioni, ottenendo l'intera quota di mercato. Con l'ingresso di una seconda azienda, lo stesso investimento aggiuntivo è meno efficace perché l'intero ricavo di mercato si ottiene

solo se il concorrente viene colpito. Dal punto di vista del benessere collettivo, l'investimento di equilibrio è al di sopra del livello sociale efficiente, ovvero le imprese investono troppo in sicurezza informatica. Questo è dovuto all'esternalità negativa prodotta dagli spillover di mercato: il beneficio marginale privato è superiore al beneficio marginale sociale perché il primo non comprende la minore probabilità della impresa che non investe di ottenere la quota di ricavi dell'impresa che effettua la spesa in sicurezza.

Se le imprese sono sia interconnesse che concorrenti, spillovers tecnici e di mercato sono contemporaneamente presenti. In questo scenario, l'incentivo al free-riding generato dai benefici tecnologici condivisi riduce l'investimento di equilibrio di un'azienda quando un'altra azienda si unisce alla rete informatica. Allo stesso modo, gli effetti di spillover nel mercato hanno un impatto negativo, poiché la probabilità che un'azienda riesca ad accaparrarsi l'intero ricavo del mercato diminuisce quando si passa da un monopolio a un duopolio: se si tiene conto di entrambi i tipi di spillover, questi due effetti negativi si sommano. Confrontando il livello socialmente efficiente con quello di equilibrio si osserva che per valori delle ricadute da spillover tecnici relativamente bassi si verifica sovrainvestimento, altrimenti le imprese sovrainvestono. L'intuizione è che l'influenza degli spillover di mercato diventa più significativa quando gli spillover tecnici hanno un basso impatto. Questa dinamica crea un effetto esterno negativo, causando una discrepanza tra il beneficio sociale dell'investimento e il beneficio privato e portando a un eccesso di investimento. Tuttavia, all'aumentare dell'impatto degli spillover tecnici, l'effetto esterno positivo correlato aumenta progressivamente e alla fine supera quello negativo prodotto dagli effetti di spillover nel mercato. Di conseguenza, il beneficio sociale supera il beneficio privato, determinando un insufficiente investimento complessivo.

Due lavori che hanno studiato gli investimenti aziendali nella cybersecurity quando l'interdipendenza delle imprese assume la forma di spillover sia tecnici che di mercato sono quelli di Liao e Chen [83] e Jianqiang et al. [84]. Liao e Chen studiano l'impatto dell'esternalità della rete sugli incentivi delle imprese a investire nella sicurezza delle informazioni. I risultati suggeriscono inoltre la chiara necessità di coordinare gli investimenti in sicurezza per ottenere il massimo beneficio. Jianqiang et al. identificano i rischi dovuti alla interconnettività delle imprese in rischio di contagio, che fanno riferimento agli effetti degli investimenti delle diverse aziende in una rete sulla probabilità di subire una violazione di un'azienda singola, e in rischio di fiducia, per cui quando un'impresa non solo subisce i danni dovuti alla perdita di dati e all'interruzione dell'attività ma anche legati alla perdita di

fiducia delle altre imprese. Analizzando una situazione di gioco non cooperativo, nel caso di duopolio simmetrico, entrambe le imprese investono ugualmente. Inoltre, il livello di investimento in sicurezza dell'impresa è decrescente in funzione del rischio infettivo e aumenta quando aumenta il rischio di fiducia. Nel caso di gioco cooperativo, l'investimento di un'azienda non aumenta monotonamente con il rischio infettivo e il rischio di fiducia, ma gli effetti di questi due fattori sull'investimento in sicurezza delle informazioni sono gli stessi. Infine, si trova il risultato apparentemente controintuitivo che le imprese che affrontano i rischi infettivi non sempre investono meno del livello socialmente efficiente: le imprese sotto investono in sicurezza, rispetto al livello di investimento quando le imprese decidono congiuntamente, quando il rischio di fiducia è sufficientemente piccolo.

2.3 Determinanti degli investimenti in sicurezza informatica

Abbiamo visto come gli investimenti in cybersecurity sono ormai parte delle decisioni strategiche che le imprese devono affrontare per poter rafforzare il monitoraggio e la difesa da minacce hacker che potrebbero compromettere il corretto funzionamento dei sistemi informativi e comportare ingenti costi, rappresentati dalla perdita di dati, di immagine o in alcuni casi anche monetari, quando ci si trova davanti ad un pagamento necessario per un eventuale riscatto.

Così come sono diventati importanti per le imprese, gli investimenti in sicurezza informatica hanno attirato anche l'attenzione di numerosi studiosi, economisti e ricercatori. Nel seguente capitolo verranno analizzati i principali risultati degli studi riguardanti l'esplorazione dei fattori che possono determinare gli investimenti in cybersicurezza nelle imprese.

Gordon et al. [85] nel 2018 hanno dimostrato che tra i driver che guidano il livello di investimento del settore privato in attività di cybersecurity si trovano l'interesse di un'impresa sul rischio di incorrere in grandi perdite a causa di una violazione della sicurezza informatica, il grado con cui tali investimenti sono considerati come fonti di vantaggio competitivo e la misura con cui la cybersecurity è vista come componente importante per la rendicontazione fiscale. Lo studio empirico è stato effettuato con una indagine sottoposta ad un totale di 2000 dirigenti senior responsabili degli aspetti tecnici degli investimenti in questione (es. Chief Information Officer o Chief Financial Officer) di circa 1600 organizzazioni degli Stati Uniti di cui sono state ottenute 158 risposte utilizzabili. Per indagare le variabili sopra indicate è stata usata la regressione seguente:

$$log\frac{prob(Bgt)}{[1-prob(Bgt)]} = \beta_0 + \beta_1 IC + \beta_2 CR + \beta_3 CA + \beta_4 Rev + \varepsilon$$

La variabile dipendente Bgt è la quota percentuale del budget IT dedicato agli investimenti in cybersecurity e le variabili indipendenti, misurate su una scala da 1 (fortemente in disaccordo) a 7 (fortemente d'accordo), sono IC, che è il livello di considerazione della cybersecurity come parte rilevante dei controlli interni dei sistemi di rendicontazione, CR, che è associata a quanto l'impresa valuta la perdita potenziale più grande quando stima il rischio della minaccia hacker, CA, che misura il riconoscimento degli investimenti come potenziale vantaggio competitivo e Rev, che si riferisce al fatturato annuo lordo. I risultati in Figura 26 permettono di valutare come le variabili indipendenti influenzino la probabilità che la variabile dipendente assuma uno specifico valore. In particolare, i coefficienti di IC e CR hanno significatività positiva al 5%, mentre quello di CA al 10%, suggerendo che un valore elevato di queste tre variabili è associato ad un livello percentuale maggiore di budget dedicato alla cybersecurity. Si osserva però che il coefficiente di Rev è significativo e negativo al livello di 1%, evidenziando come le imprese con un fatturato maggiore dedicano una percentuale minore di budget alla sicurezza informatica.

Independent variables	Coefficient	P-value	Odd ratio estimates
IC	0.2688	0.0410	1.308
CR	0.2337	0.0198	1.263
CA	0.1744	0.0707	1.191
Rev	−0.4939	0.0005	0.610

Figura 26. Risultati dello studio di Gordon et al. [85]

De Arroyabe et al. [86] nel 2023 hanno analizzato come le capacità informatiche e gli attacchi informatici subiti da un'impresa guidano gli investimenti nei sistemi di cybersicurezza. La ricerca è stata effettuata su un campione di 4.163 organizzazioni del Regno Unito i cui dati sono stati forniti dalla Cyber Security Breaches Survey del 2018-2019 e sono state usate tecniche di machine learning come ANN[10] (Artificial Neural Network) e K-Means Clustering[11]. Il loro studio ha analizzato come variabile dipendente l'investimento nella cybersecurity delle organizzazioni domandando le spese sostenute in software, hardware, personale e outsourcing al fine di prevenire o identificare violazioni di sicurezza

[10] Le reti neurali, note anche come reti neurali artificiali (ANN – Artificial Neural Network), sono un sottoinsieme dell'apprendimento automatico e sono il cuore degli algoritmi di deep learning.

[11] Il clustering K-means è uno dei più semplici e popolari algoritmi di apprendimento automatico non supervisionato.

informatica. Per quanto riguarda le variabili indipendenti sono state divise tra quelle relative alle capacità e quelle riferite alle minacce informatiche. Nel primo gruppo si trovano le risorse dedicate alla gestione della cybersecurity (RESOURCES), le procedure volte alla protezione informatica condotte dalle organizzazioni (PROCEDURES) e le regole utilizzate per far fronte alle minacce cyber (RULES). Nel secondo gruppo, invece, fanno parte la tipologia (TYPOLOGY OF ATTACKS) e la frequenza degli attacchi informatici subiti dall'impresa (FREQUENCY OF ATTACKS). Per testare ulteriormente la domanda di ricerca è stata utilizzata anche una regressione logit ordinaria, i cui risultati sono mostrati nella Figura 27.

Variables	2019				VIF	2018				VIF
	Estimate	Std. Error	Estimate	Std. Error		Estimate	Std. Error	Estimate	Std. Error	
RESOURCES			.330***	.060	1.543			.404***	.057	1.758
PROCEDURES			.352***	.057	1.571			.346***	.055	1.794
RULES			.250***	.054	1.413			.215***	.044	1.673
ATTACK			.271***	.059	1.074			.255***	.053	1.126
FREQUENCY	.058	.042	.024	.047	1.018	−0.007	.012	.025	.043	1.019
−2 Log-Likelihood	282.956		2414.409			279.023		2781.302		
Chi-Square	1.902		277.099			.256		399.353		
Df	1		5			1		5		
Sig.	.000		.000			.613		.000		
Cox and Snell	.002		.345			.000		.407		
Nagelkerke	.003		.350			.000		.412		
McFadden	.001		.098			.000		.120		

*** *p<0.001*, ** *p<0.005*, * *p<0.01*.Durbin-Watson (2019): 1.879; Durbin-Watson (2018): 1.783.

Figura 27. Risultati dello studio di De Arrobaye et al. [86]

I risultati mostrano che la variabile di frequenza non è significativa in entrambi i casi permettendo di concludere che non influisce direttamente sugli investimenti. Al contrario, le risorse, le procedure, le regole e il tipo di attacchi condizionano la decisione di investire in sistemi di cybersecurity e risultano significative e positive al livello di 1%.

Nello studio di Tomaso Duso e Alexander Schiersch [87] effettuato sui dati di un campione di aziende tedesche per gli anni 2014 e 2016 viene dimostrato come l'adozione del cloud, nonostante sia uno strumento in grado di migliorare l'utilizzo delle aziende delle soluzioni IT, non impatta gli investimenti IT in nessun settore. Al contrario, migliora la produttività del lavoro nel settore manifatturiero e dei servizi di informazione e comunicazione. L'analisi tiene conto anche della disponibilità della banda larga a 16 Mbp/s a livello municipale che risulta essere un driver nella scelta dell'adozione del cloud, ma solo nel settore manifatturiero. I risultati relativi al settore manifatturiero, ottenuti attraverso una regressione probit e mostrati in Figura 28, evidenziano che la probabilità di usufruire di servizi di cloud computing è maggiore per le imprese più grandi, dimostrando una correlazione positiva tra adozione del cloud e dimensione dell'impresa, e più favorevoli alle soluzioni digitali visto il loro livello tecnologico, determinate dalla presenza di staff IT qualificato e disponibilità di

capacità IT. Infatti, il capitale informatico è significativo solo nelle prime stime e perde significatività quando viene aggiunta la variabile sul personale IT. Inoltre, la quota di vendite avvenute tramite Internet sembra essere un buon predittore degli investimenti in cloud computing. Relativamente ai servizi, invece, le dimensioni d'azienda non sono significative e, allo stesso modo, la presenza della banda larga. Si rileva che la presenza di personale specializzato e le vendite web rimangono significative per le imprese di servizi di informazione, di comunicazione e di business aziendale.

	(1)	(2)	(3)	(4)	(5)	(7)	(8)	(9)
Variable	manufacturing					inform. &com. serv.	business serv.	other serv.
Broadband$_t$	0.00318**	0.00316**	0.00317**	0.00321**	0.00334**	−0.00185	−0.00498	0.00168
	(0.00153)	(0.00154)	(0.00153)	(0.00154)	(0.00155)	(0.00342)	(0.00418)	(0.00435)
Labor$_{t-1}$	0.412***	0.343***	0.301***	0.271***	0.262***	0.0500	−0.0907	0.0659
	(0.0327)	(0.0438)	(0.0836)	(0.0844)	(0.0850)	(0.0892)	(0.0875)	(0.121)
IT Capital$_{t-1}$		0.0533**	0.0505**	0.0399	0.0378	0.0465	0.0805**	0.0461
		(0.0234)	(0.0238)	(0.0245)	(0.0246)	(0.0314)	(0.0359)	(0.0436)
Tang.Capital$_{t-1}$			0.0417	0.0423	0.0454	−0.0634	−0.0565	0.0880
			(0.0694)	(0.0697)	(0.0701)	(0.0793)	(0.0631)	(0.0751)
IT Staff$_t$				0.278***	0.280***	0.634***	0.400**	0.357**
				(0.0991)	(0.0995)	(0.206)	(0.157)	(0.179)
Perc. Web Sales$_t$					0.0151***	0.00611*	0.0199***	0.00393
					(0.00416)	(0.00361)	(0.00482)	(0.00545)
Constant	−2.573***	−2.801***	−3.192***	−3.093***	−3.017***	−0.777	−0.279	−2.083**
	(0.420)	(0.430)	(0.766)	(0.772)	(0.776)	(1.118)	(1.011)	(1.027)
N	1,860	1,860	1,860	1,860	1,860	500	476	368

Figura 28. Risultati dello studio di Tomaso Duso e Alexander Schiersch [87]

Indagando la correlazione tra gli investimenti IT e il cloud computing, è emerso che l'utilizzo dei servizi cloud non è correlato agli investimenti. Nel settore manifatturiero, i determinanti delle spese IT sono lo stock di capitale informatico e tangibile. È evidente come il coefficiente della variabile cloud diventa insignificante dopo aver preso in considerazione la variabile sul capitale IT dell'azienda dell'anno precedente, non portando alla luce prove del fatto che l'uso del cloud è un sostituto dell'investimento interno in tecnologie IT. A differenza del manifatturiero, in nessuno dei settori dei servizi il capitale tangibile ha una correlazione significativa con gli investimenti IT (vedi Figura 29).

variables	(1)	(2)	(3)	(4)	(5) inform. &com. services	(6) business services	(7) other services
	manufacturing						
Cloud Comp.$_t$	2.183***	0.667**	0.395	0.313	0.434	0.478	0.441
	(0.282)	(0.273)	(0.246)	(0.246)	(0.427)	(0.506)	(0.557)
Tang.Capital$_{t-1}$		1.595***		0.195*	−0.112	0.216	−0.137
		(0.0810)		(0.106)	(0.183)	(0.156)	(0.226)
IT-Capital$_{t-1}$			1.408***	1.326***	1.350***	0.914***	1.085***
			(0.0475)	(0.0677)	(0.103)	(0.0942)	(0.127)
Constant	4.717***	−20.87***	−11.09***	−13.30***	−6.296*	−12.14***	−1.060
	(1.766)	(2.053)	(1.505)	(1.892)	(3.694)	(3.046)	(3.987)
R^2	0.076	0.220	0.357	0.358	0.398	0.374	0.312
N	1,860	1,860	1,860	1,860	500	476	382

Figura 29. Risultati dello studio di Tomaso Duso e Alexander Schiersch [87]

Un importante contributo alla ricerca è quello di Shaik e Siponen [88] che indaga come i costi delle violazioni informatiche provocano un aumento degli investimenti in cybersecurity di un'impresa, andando a valutare inoltre la fonte di identificazione della minaccia cyber tra interna o esterna. Lo studio è stato effettuato su 722 aziende del Regno Unito, con 267, 252 e 203 osservazioni rispettivamente negli anni 2018, 2019 e 2020, e dimostra che costi delle violazioni più alti hanno maggiori probabilità di generare un aumento degli investimenti e tale effetto è rafforzato ulteriormente se la violazione è identificata da una terza parte. Il modello testato valuta come variabile dipendente l'investimento in cybersecurity, codificata come 1 se le aziende hanno aumentato la spesa in sicurezza informatica e 0 altrimenti. La variabile indipendente è data dal costo della violazione, misurata in una scala da 1 a 12 che comprende un costo che va da meno di 100 sterline a più di cinque milioni di sterline. Come anticipato, è valutata la fonte di identificazione della violazione con una variabile codificata come 1 se la violazione è osservata internamente e 0 se esternamente da terzi. Le variabili di controllo utilizzate sono la dimensione dell'azienda valutata con il numero di dipendenti, il settore industriale, la presenza online delle imprese e il tipo di violazione. Infine, si controllano gli effetti fissi dell'anno. È stata utilizzata una regressione logistica e l'equazione che mostra il modello è la seguente:

$$CybersecurityInvestment = \beta_1 BreachCost + \beta_2 BreachCost * BreachIdentificationSource + \gamma Controls + \eta_t + \mu$$

I test di ipotesi con regressione logistica sono effettuati con quattro modelli (vedi Figura 30). Nel modello 1 sono incluse sono le variabili di controllo. Nel modello 2 viene aggiunta la variabile sul costo di violazione e il suo effetto sull'investimento in cybersecurity è significativo e positivo. Nel modello 3 viene incluso anche l'effetto della fonte di

identificazione ma non si osserva nessun effetto statisticamente significativo. Nel modello 4, che è quello completo di tutte le variabili, rimane positivo e significativo l'effetto dei costi e, inoltre, si conferma l'effetto moderatore della fonte di identificazione della violazione. L'analisi empirica evidenzia che le violazioni che comportano maggiori costi comportano una maggiore probabilità di aumentare gli investimenti in cybersecurity. Questa probabilità aumenta in caso di una più debole capacità di risposta agli incidenti, rappresentata dalle violazioni segnalate da terzi.

Variables	Hypothesis	Model 1		Model 2		Model 3		Model 4	
DV: Cybersecurity investment		B	S.E	B	S.E	B	S.E	B	S.E
Firm size		0.095	0.120	0.197	0.182	0.198	0.189	0.204	0.191
Online presence		0.195	0.141	-0.142	0.191	-0.228	0.189	-0.236	0.190
Ransomware		0.408	0.815	-0.545	0.913	-0.615	0.936	-0.542	0.919
Malware		-0.648	0.893	-1.171	1.051	-1.207	1.060	-1.278	1.088
Denial of service		0.629	0.826	0.687	0.884	0.606	0.884	0.728	0.895
Bank account hacking		-0.019	1.041	-0.433	1.298	-0.531	1.320	-0.463	1.297
Impersonation		-0.340	0.790	-0.422	0.901	-0.539	0.931	-0.593	0.938
Phishing		-1.133	0.778	-1.899**	1.027	-2.643**	1.202	-2.762**	1.234
Unauthorized file/ network access (Insider)		0.830	1.029	0.000	0.000	0.000	0.000	0.000	0.000
Unauthorized file/ network access (Outsider)		0.456	0.884	-0.785	1.102	-0.980	1.120	-1.060	1.179
Breach costs	H1(+)			0.237***	0.099	0.228**	0.106	0.522***	0.192
Breach identification source						-0.453	0.507	1.665	1.328
Breach costs x Breach identification source	H2(+)							-0.409**	0.240
Constant		-3.706***	0.951	-3.521***	1.239	-3.109**	1.388	-4.672***	1.496

*** $p<0.01$, ** $p<0.05$, * $p<0.1$

Controls for Year and Industry included

Figura 30. Risultati dello studio di Shaik e Siponen [88]

Gatzert, Nadine e Schubert [89] hanno effettuato un'analisi empirica sulle imprese del settore bancario e assicurativo negli Stati Uniti dal 2011 al 2018 riguardo alla consapevolezza, alle determinanti e al valore della gestione del rischio di natura cyber (che loro chiamano CyberRM – Cyber Risk Management). In questo caso non si valuta la spesa in sicurezza informatica ma piuttosto la scelta di un'impresa ad attuare la gestione del rischio informatico, che comporta investimenti in cybersicurezza. La consapevolezza del rischio cyber è misurata attraverso un punteggio ottenuto attraverso un algoritmo di text mining basato su regole applicate alle relazioni annuali 10-K sottoposte alle aziende del campione. I risultati di questa prima ricerca evidenziano l'aumento del punteggio della consapevolezza del rischio cyber nel settore bancario e assicurativo nel periodo di campionamento. Distinguendo i due settori, il settore assicurativo ha punteggio medi più alti rispetto a quello bancario. I fattori determinanti del CyberRM di cui viene studiato l'impatto sono la dimensione dell'impresa, la leva finanziaria, il rendimento delle attività (RoA), la Capital Opacity determinata dal rapporto tra le attività immateriali rispetto al valore contabile delle

attività totali, il settore (bancario o assicurativo), la consapevolezza del rischio informatico utilizzando il punteggio calcolato in precedenza, la consapevolezza del rischio in generale misurato calcolando il numero di volte che appare il termine "rischio" nelle relazioni annuali. La variabile dipendente è rappresentata dalla probabilità che un'azienda abbia implementato il CyberRM e il modello è espresso come segue:

$$\ln\left(\frac{p(CyberRM=1)}{1-p(CyberRM=1)}\right) = \beta_1 Size + \beta_2 Leverage + \beta_3 RoA + \beta_4 CapitalOpacity + \beta_5 Bank + \beta_6 CyberRiskAwareness + \beta_7 RiskAwareness + \beta_{8-14} YearDummies + \varepsilon$$

Dall'analisi di regressione svolta su tutte le imprese emerge che le imprese più redditizie (maggiore RoA) hanno una minore probabilità di adottare il CyberRM. Al contrario, le imprese bancarie, con maggiore consapevolezza del rischio informativo e del rischio generale hanno una maggiore probabilità di implementare il CyberRM. I risultati sulla dimensione, leva finanziaria e opacità del capitale non sono statisticamente significativi per l'intero campione analizzato. Andando a condurre due regressioni separate per banche e assicurazioni, l'impatto di CyberRiskAwareness e di RiskAwareness è statisticamente positivo per entrambi i settori. Inoltre, si osserva un effetto statisticamente negativo del RoA e della dimensione nel settore assicurativo.

Infine, lo studio si propone di valutare l'impatto del CyberRM sul valore dell'impresa ed emerge una relazione positiva e statisticamente significativa. Valutando l'intero campione di imprese, si osserva che le aziende con CyberRM hanno un valore più alto del 10,92% rispetto a quelle senza. Osservando i due campioni separatamente, l'effetto positivo è maggiore per le imprese assicurative (19,98%) rispetto a quelle bancarie (6,37%).

Lo studio di Biancotti C. [90] effettuato nel 2017, sulla base delle indagini annuali della Banca d'Italia del 2016 sulle imprese private dell'industria e dei servizi non finanziari con almeno 20 dipendenti che raccolgono per la prima volta informazioni riguardo al tema della cybersecurity nel territorio italiano, indaga i determinanti dell'adozione delle misure difensive e della spesa in sicurezza informatica. I risultati riportano che la spesa media nel 2016 è stata di 4.530 euro, con differenze tra le dimensioni d'impresa (si osserva un valore medio di 3.120 euro per le piccole imprese e 44.590 euro per le grandi imprese) e tra i settori (si osserva un valore medio di 3.240 nei settori a bassa tecnologia e 19.080 euro nel settore ICT), e che il mercato di riferimento vale almeno 570 milioni di euro. La ricerca dimostra che un'impresa che è stata bersaglio di un attacco informatico è incentivata ad investire in cybersecurity. Infatti, l'81% di queste imprese ha aggiornato le proprie difese. Per quanto

riguarda la dimensione dei danni subiti emerge che la maggior parte delle aziende ha subito danni inferiori a 10.000 euro, circa l'1% superiori a 50.000 euro e lo 0,1% almeno di 200.000 euro. Il campione analizzato è formato da 3824 imprese e le domande della sezione sulla sicurezza informatica chiedono quali misure in cybersecurity sono incluse nell'azienda, quale è stata la spesa in cybersicurezza, la segnalazione di un attacco informatico, le conseguenze e i danni di tale attacco e, infine, l'indicazione di un rafforzamento delle misure di sicurezza. I risultati descrittivi principali riportano che il 99% delle aziende segnala l'adozione di software o hardware difensivi, la formazione sulla cybersecurity per i dipendenti è diffusa nel 65% delle aziende, l'analisi e la gestione delle vulnerabilità nel 56,9% e la crittografia nel 32,7%. Si osserva che la prevalenza di queste misure aumenta con le dimensioni dell'impresa. Anche dai risultati della analisi di regressione lineare in Figura 31 emerge che le dimensioni, la maturità tecnologica e lo status di attacco hanno un impatto sulle scelte difensive: un'impresa del settore ICT impiega 1,15 misure in più, mentre quelle che hanno subito un attacco rafforzano le difese con 0,41 misure. Il Sud Italia ha un livello di protezione inferiore rispetto al resto del Paese; al contrario, gli esportatori e le imprese che gestiscono infrastrutture hanno maggiori difese.

Una ulteriore regressione logistica, i cui risultati sono mostrati in Figura 32, conferma che, anche dopo aver controllato tutti gli altri fattori, le piccole imprese e quelle a bassa tecnologia spendono meno, mentre il settore ICT spende di più.

Intercept	2.910	***
	(0.054)	
Small	-0.409	***
	(0.038)	
South	-0.140	**
	(0.046)	
ICT	1.147	***
	(0.090)	
High-tech non-ICT	0.312	***
	(0.043)	
Manufacturing	-0.334	***
	(0.038)	
Export share: less than 1/3	-0.175	***
	(0.044)	
Infrastructure	0.315	**
	(0.129)	
Attacked, upgraded defences	0.409	***
	(0.044)	
Attacked, did not upgrade defences	-0.102	
	(0.085)	
N	3,456	
R^2	0.14	

Figura 31. Risultati dello studio di Biancotti C. [90]

Small	-3.635	***
	(0.070)	
Medium (low)	-2.527	***
	(0.070)	
Medium (high)	-1.531	***
	(0.079)	
South	-0.434	***
	(0.034)	
ICT	2.313	***
	(0.050)	
High-tech non-ICT	0.539	***
	(0.028)	
Manufacturing	-0.228	***
	(0.026)	
Infrastructure	0.870	***
	(0.073)	
Attacked, upgraded defences	0.311	***
	(0.027)	
Attacked, did not upgrade defences	-0.460	***
	(0.064)	
Turnover per employee	$5.38*10^{-4}$	***
	$(2.20*10^{-5})$	
Turnover per employee squared	$-1.23*10^{-8}$	***
	$(6.44*10^{-10})$	
Export share: less than 1/3	-0.280	***
	(0.029)	
Intercept: 200,000+	-2.379	***
	(0.082)	
Intercept: 50,000-199,999	-0.700	***
	(0.072)	
Intercept: 10,000-49,999	1.887	***
	(0.074)	
N	3,005	

Figura 32. Risultati dello studio di Biancotti C. [90]

2.4 Determinanti dei costi e delle cause degli attacchi informatici

Oltre a valutare i determinanti degli investimenti in cybersicurezza, alcuni studi hanno tentato di indagare i fattori che determinano i costi informatici dovuti ad incidenti cyber. Tra questi troviamo il lavoro di Aldasoro, Inaki et al. [91] che studia i fattori che contribuiscono ai costi delle violazioni cyber, gli effetti dell'utilizzo di servizi cloud e delle tecnologie digitali sui costi informatici e, infine, l'impatto degli investimenti IT sui costi degli incidenti informatici. Per quanto riguarda i driver dei costi analizzati in Figura 33, la dimensione dell'azienda (misurata in termini di ricavi totali) è positivamente correlata al costo medio di un evento suggerendo che imprese più grandi tendono a sostenere costi maggiori, per cui l'aumento dell'1% della dimensione comporta un aumento del costo del 0,23%. Gli eventi connessi (connected events), che indicano il numero di imprese collegate ad uno specifico incidente di hacking, sono positivamente significativi per cui un aumento unitario del numero di imprese colpite si traduce in un aumento del 2,6% dei costi. Se si valuta la differenza tra attacchi informatici dolosi e non dolosi, si osserva che gli eventi malevoli (malicious) sono associati a un costo inferiore. Inoltre, per quanto riguarda i tipi di incidenti, notiamo che gli incidenti di tipo Other e Phishing/Skimming sono in media più costosi.

Dependent variable: Log(Cost)				
Regressor	I	II	III	IV
log(Firm size)	0.241***	0.220***	0.231***	0.220***
	(0.0300)	(0.0228)	(0.0234)	(0.0222)
Connected events	0.0176**	0.0257***	0.0257***	0.0238***
	(0.00740)	(0.00555)	(0.00548)	(0.00661)
Malicious	−1.31***	−1.33***	−1.20***	−1.09***
	(0.230)	(0.179)	(0.207)	(0.324)
Security incident	11.0***	13.0***	13.6***	13.8***
	(0.338)	(0.631)	(0.676)	(0.632)
Data breach	11.6***	14.1***	14.6***	14.8***
	(0.186)	(0.469)	(0.477)	(0.603)
Phishing/Skimming	12.7***	14.7***	15.1***	15.4***
	(0.486)	(0.573)	(0.554)	(0.683)
Privacy violation	10.8***	13.2***	14.0***	14.3***
	(0.387)	(0.708)	(0.755)	(0.701)
Other	12.6***	14.4***	15.3***	15.2***
	(0.405)	(0.636)	(0.666)	(0.895)
Year fixed effects	N	Y	Y	Y
Sector fixed effects	N	N	Y	N
Sub sector fixed effects	N	N	N	Y
R^2	0.11	0.19	0.21	0.25
N	3705	3705	3705	3705

Figura 33. Risultati dello studio di Aldasoro, Inaki et al. [91]

I risultati riguardanti l'utilizzo di tecnologie cloud, in Figura 34, suggeriscono che una loro maggiore implementazione porta ad una mitigazione dei costi derivanti da incidenti informatici. Una maggiore quota di servizi digitali considerata isolatamente non ha un effetto statisticamente significativo, mentre con l'aggiunta del termine di interazione con la dimensione d'impresa si trova un effetto di attenuazione dei costi.

Dependent variable: Log(Cost)					
Regressor	I	II	III	IV	V
log(Firm size)	0.222***	0.221***	0.220***	0.454***	0.450***
	(0.0224)	(0.0224)	(0.0228)	(0.128)	(0.126)
Connected events	0.0256***	0.0256***	0.0258***	0.0253***	0.0254***
	(0.00550)	(0.00549)	(0.00549)	(0.00523)	(0.00525)
Share of digital		−0.0142	0.0554	0.0461	0.114*
		(0.0445)	(0.0484)	(0.0631)	(0.0671)
log(Firm size) × Share of digital				−0.0156*	−0.0154*
				(0.00858)	(0.00846)
Share of cloud	−0.0211		−0.0378**		−0.0371*
	(0.0154)		(0.0188)		(0.0198)
Malicious	−1.33***	−1.33***	−1.33***	−1.34***	−1.34***
	(0.172)	(0.173)	(0.171)	(0.171)	(0.169)
Year fixed effects	Y	Y	Y	Y	Y
Sector fixed effects	N	N	N	N	N
Case type fixed effects	Y	Y	Y	Y	Y
R^2	0.19	0.19	0.19	0.19	0.20
N	3705	3705	3705	3705	3705

Figura 34. Risultati dello studio di Aldasoro, Inaki et al. [91]

Per valutare se gli investimenti IT possono contribuire alla mitigazione dei costi informatici vengono analizzati dati di 500 aziende con sede negli Stati Uniti in vari settori raccolti dall'indagine Information Week IW500[12]. I risultati delle regressioni che utilizzano la misura della spesa contemporanea indicano nessun effetto della spesa sui costi degli incidenti informatici, come si può vedere in Figura 35. Tuttavia, se si include il ritardo, si osserva un impatto negativo (ossia un effetto di attenuazione), evidenziando come un aumento dell'1% della spesa IT è correlato a una diminuzione del 34% dei costi. Si osserva, inoltre, che l'effetto della spesa si rafforza anche per gli incidenti dolosi.

Dependent variable: Log(Cost)					
Regressor	I	II	III	IV	V
log(Firm size)	0.228***	0.228***	0.228***	0.228***	0.230***
	(0.0232)	(0.0232)	(0.0197)	(0.0197)	(0.0190)
Connections	0.0159	0.0159	0.0245***	0.0245***	0.0251***
	(0.0101)	(0.0101)	(0.00679)	(0.00679)	(0.00708)
Malicious	−1.12***	−1.12***	−1.02***	−1.02***	
	(0.350)	(0.350)	(0.288)	(0.288)	
IT spending	−29.2	−29.2			
	(30.5)	(30.5)			
IT spending lag			−41.3*	−41.3*	−35.6*
			(22.6)	(22.6)	(21.5)
IT spending lag × Malicious					−22.9***
					(7.69)
Share of cloud		0.0217		−1.13***	−1.13***
		(0.158)		(0.135)	(0.128)
Share of digital		−0.286		1.34***	1.37***
		(0.188)		(0.152)	(0.153)
Year fixed effects	Y	Y	Y	Y	Y
Sector fixed effects	Y	Y	Y	Y	Y
Case type fixed effects	Y	Y	Y	Y	Y
R^2	0.2	0.2	0.2	0.2	0.21
N	2611	2611	2953	2953	2953

Figura 35. Risultati dello studio di Aldasoro, Inaki et al. [91]

Un altro studio che contribuisce all'esplorazione delle cause degli attacchi cyber è quello di Caldarulo et al. [92] nel quale vengono analizzate come variabili dipendenti le cause delle violazioni della sicurezza e quelle della divulgazione non autorizzata di dati nelle organizzazioni pubbliche con due modelli di regressione basati sui dati provenienti da un sondaggio nazionale somministrato nel 2018 a dirigenti pubblici di 500 città degli Stati Uniti di piccole e medie dimensioni. I fattori che determinano le variabili dipendenti vengono

[12] InformationWeek è una rivista digitale che fornisce una piattaforma per i leader dell'IT aziendale e le aziende tecnologiche leader per condividere le loro intuizioni ed esperienze attraverso interviste esclusive, articoli di opinione ed eventi, offrendo testimonianze di prima mano su strategie, tendenze e innovazioni.

suddivisi in organizzativi e ambientali e i risultati mostrano come entrambi siano determinanti degli incidenti informatici. Tra i fattori organizzativi sono individuati la centralizzazione, la cultura orientata al rischio, il numero di canali di comunicazione IT e la capacità IT, mentre tra quelli ambientali si trovano la forma di governo (mayor-council o council-manager), la competizione politica misurata con il numero di cambi di partito nelle ultime 10 elezioni, la disuguaglianza economica, l'eterogeneità razziale e la dimensione delle città. Le variabili di controllo analizzate riguardano il tipo di dipartimento e le sue dimensioni, e il numero di anni in cui gli intervistati lavorato nel settore privato. Per quanto riguarda le variabili dipendenti dei due rispettivi modelli, dei 578 intervistati il 45,25% ha segnalato violazioni della sicurezza che indicano gli incidenti informatici causati da esterni mentre il 10% circa ha subito divulgazioni non autorizzate di dati che sono causate da attori interni. I risultati dei determinanti organizzativi mostrano come i dipartimenti con maggiori canali di comunicazione IT hanno maggiore probabilità di subire attacchi informatici, mentre quelli con livelli più alti di capacità informatica sono meno propensi a segnalare un incedente informatico. La centralizzazione e la cultura del rischio non hanno portato a risultati statisticamente significativi. Guardando ai fattori ambientali, le città con forma di governo comunale (council-manager) hanno minore probabilità di subire una violazione delle sicurezza, mentre non è riscontrata alcuna relazione significativa con la segnalazione di divulgazione di dati non autorizzata. Inoltre, è evidenziata una relazione negativa e statisticamente significativa tra il numero di cambi di partito nelle ultime 10 elezioni e la segnalazione di violazioni della sicurezza. La competizione politica, misurata dal margine di voto tra i partiti, è statisticamente correlata positivamente con le divulgazioni di dati non autorizzate. Le variabili della disuguaglianza economica, dell'eterogeneità razziale e della dimensione della città non hanno mostrato risultati statisticamente significativi. I risultati appena citati sono visibili in Figura 36.

Parameter	Security Breaches			Unauthorized Data Disclosures		
	β	AME	Std. Error	β	AME	Std. Error
Organizational Factors						
Centralization	−0.056	−0.014	0.182	0.073	0.005	0.292
Risk-Taking	−0.121	−0.030	0.176	−0.384	−0.028	0.276
Number of IT Communication Channels	0.218***	0.054	0.062	0.161*	0.012	0.093
IT Capacity	−0.309**	−0.077	0.141	−0.446**	−0.033	0.222
Environmental Determinants						
Council-Manager	−0.670**	−0.160	0.296	0.135	0.010	0.407
# Partisan Shifts in the last 10 elections (ln)	−0.488*	−0.121	0.292	0.494	0.037	0.441
Margin of Partisan Vote	−0.438	−0.108	1.422	3.221*	0.238	1.912
Gini Coefficient	1.198	0.297	4.052	7.515	0.556	6.482
Lieberson Index of Inequality	−1.152	−0.286	0.943	−1.126	−0.083	1.350
Population (2017) (ln)	0.302	0.075	0.194	0.326	0.024	0.320
Control Variables						
Mayor's office	1.017***	0.248	0.377	−0.115	−0.008	0.483
Community Development Department	0.671*	0.166	0.404	−0.620	−0.040	0.564
Finance Department	1.619***	0.378	0.405	−0.114	−0.008	0.639
Parks Department	0.688*	0.170	0.383	−1.353**	−0.074	0.609
Full-Time Employees (ln)	0.008	0.002	0.088	0.085	0.006	0.137
Years of Experience in the Private Sector	0.025	0.006	0.019	−0.053*	−0.004	0.028
Intercept	−3.390		2.746	−6.960		4.683
Nagelkerke R Square	0.177			0.148		
N	393			468		

Figura 36. Risultati dello studio di Caldarulo et al. [92]

Sasha Romanosky [93] ha esaminato i costi e la cause degli incidenti cyber esaminando un campione di oltre 12.000 eventi informatici fornito da Advisen distinguendoli in quattro tipi differenti (violazioni di dati, incidenti di sicurezza, violazioni della privacy e incidenti di phising/skimming) ed esaminando come metriche il numero totale di incidenti, il tasso di incidenti, il tasso di controversie, il costo totale e il costo per evento. Dal set di dati che fa riferimento ad un periodo di 10 anni dal 2005 al 2014 emerge che le violazioni dei dati sono le più comuni e che tutti gli eventi sono in aumento anche se a ritmo decrescente, come mostrato in Figura 37.

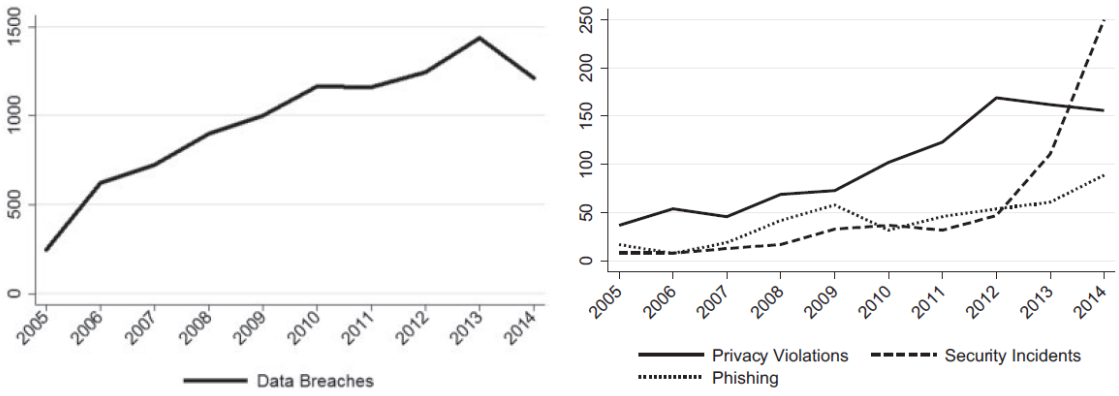

Figura 37. Andamento negli anni delle violazioni della sicurezza informatica [93]

Esaminando gli incidenti e i tassi di incidenza per settore si scopre che i settori finanziario e assicurativo, sanità e Pubblica Amministrazione hanno subito il maggior numero di violazioni, seguiti dai servizi educativi, produzione e i servizi di informazione. Il secondo obiettivo dello studio è quello di sviluppare un modello che permetta di studiare i fattori che determinano i costi, e quello proposto è il seguente:

$$log(cost_{it}) = \beta_0 + \beta_1 log(revenue_{it}) + \beta_2 log(records_{it}) + \beta_3 repeat_{it} + \beta_4 malicious_{it} + \beta_5 lawsuit_{it} + \alpha FirmType_{it} + \lambda_t + \rho_{ind} + \mu_{it}$$

dove $cost_{it}$ è il costo totale dell'incidente sostenuto dall'impresa i nell'anno t, $revenue_{it}$ è il log del fatturato dell'azienda, $records_{it}$ è il numero di record compromessi dall'incidente, $repeat_{it}$ è una variabile binaria codificata come 1 se l'azienda ha subito più eventi e 0 altrimenti, $malicious_{it}$ è una variabile binaria codificata come 1 se l'evento è stato causato da un intento malevolo, $lawsuit_{it}$ è una variabile binaria codificata come 1 se l'evento è stato causato da un'azione legale, $FirmType_{it}$ è un vettore di variabili binarie che descrivono se l'azienda colpita è un'agenzia governativa, un'organizzazione non profit, un'azienda privata o quotata in borsa. Sono inclusi anche vettori di variabili binarie relative all'anno e al settore, rappresentate da λ_t e ρ_{ind}.

Il modello è stimato solo per le violazioni dei dati e i risultati sono esposti in Figura 38. Questi suggeriscono che il ricavi sono associati fortemente al costo informatico di un incidente per cui un aumento del 10% dei ricavi porta ad un aumento dell'1,3% del costo. Anche il numero di record è risultato un fattore correlato al costo per cui un aumento del 10% del numero di record compromessi comporta un aumento del 2,9% dei costi. Il fatto che l'impresa abbia subito più incidenti non incide significativamente sul costo dell'incidente. Inoltre, la ricerca misura che il costo totale nei 10 anni è stato di 85.000 milioni di dollari e quindi, in media, circa 8,5 milioni di dollari all'anno. Un metodo successivamente seguito nello studio è quello di valutare i costi come percentuale dei ricavi dell'azienda ed emerge che gli incidenti informatici costano alle aziende solo lo 0,4% del loro fatturato annuale.

Dep var: log(costs)	Data breaches
Log(revenues)	0.133**
	(0.0592)
Log(records)	0.294***
	(0.0386)
Repeat player	−0.352
	(0.386)
Malicious	−0.0294
	(0.369)
Lawsuit	0.444
	(0.351)
Government	−1.339
	(1.482)
Private	−1.032
	(1.145)
Public	−0.0654
	(1.156)
Constant	−3.858*
	(2.044)
Observations	265
R^2	0.466
Year controls	Yes
Industry controls	Yes

Figura 38. Risultati dello studio di Sasha Romanosky [93]

Infine, in Figura 39 viene valutata la differenza tra i costi degli incidenti informatici e la spesa per la sicurezza informatica con un istogramma in cui i valori a sinistra dello zero corrispondono a costi superiori alla spesa IT, mentre quelli a destra il contrario. Si osserva una grande frequenza vicina allo zero che fa intendere come quasi la metà degli eventi informatici costa a un'impresa un importo approssimativamente pari all'investimento annuale in sicurezza informatica.

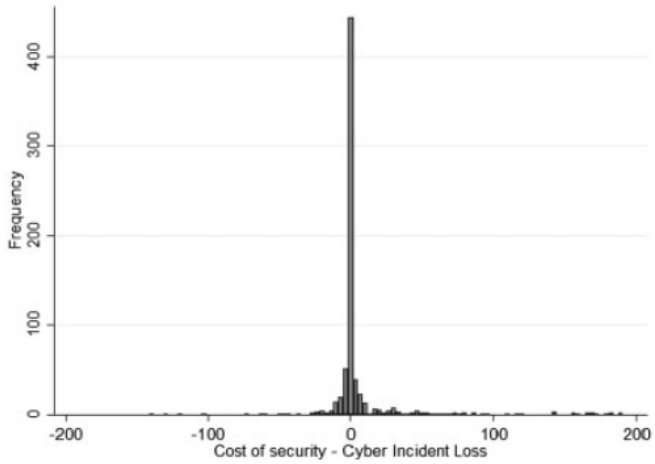

Figura 39. Differenza tra costo informatico e spesa per la sicurezza informatica [93]

Biancotti C. [94], precedentemente allo studio sugli investimenti in cybersecurity citato nel capitolo precedente, aveva già indagato il settore privato italiano. I dati di questo studio sono riferiti al corso del 2016, a differenza di quello successivo che fa riferimento all'intero anno,

e l'indagine prevedeva una domanda su come fosse gestita la cybersecurity (1 = gestita da risorse interne; 2 = esternalizzata a una società esterna, appartenente allo stesso gruppo; 3 = Esternalizzata a una società esterna, non appartenente allo stesso gruppo; 4 = Gestita in parte da risorse interne, parzialmente in outsourcing; 5 = Non applicabile, in quanto non esistono attività di cybersecurity; 9 = Non so / mi rifiuto di rispondere) e una sul numero di attacchi informatici subiti (1 = Nessun attacco; 2 = Un attacco; 3 = Tra 2 e 5 attacchi; 4 = Tra 6 e 10 attacchi; 5 = Più di 10 attacchi; 9 = Non so / mi rifiuto di rispondere). La prima domanda è stata posta per colmare la mancanza di informazioni sul modo in cui la sicurezza informatica venisse gestita nel Paese, mentre la probabilità di subire almeno un attacco è stata utilizzata come variabile dipendente nel modello di regressione sviluppato nello studio. In seguito alla pulizia del campione non considerando gli intervistati non rispondenti o che hanno riportato di non aver subito attacchi e che soddisfano un criterio scelto per la bassa capacità di rilevamento (nessuna conoscenza del TTIP - Transatlantic Trade and Investment Partnership), i dati evidenziano che il 45,2% delle aziende ha subito almeno un attacco e che gli attacchi avvengono con maggiore frequenza nelle imprese di grandi dimensioni (62,8%) e minore nelle regioni del Sud (35,9%). Valutando il livello tecnologico delle aziende, emerge che le aziende altamente tecnologiche hanno maggiore probabilità di essere bersaglio di minacce informatiche rispetto a quelle meno tecnologiche, rispettivamente con tassi del 48,8% e 43,8%. Inoltre, le imprese con una quota di esportazioni maggiore subiscono più probabilmente una violazione informatica rispetto a quelle che esportano meno. La variabile dipendente da indagare è la probabilità di essere colpiti da un attacco informatico e le variabili usate nella regressione sono riportate di seguito in Figura 40.

Descriptor	*Type*	*Content*
Small	Binary	Number of employees between 20 and 49, 2015 average
South	Binary	Administrative headquarters located in Southern Italy or Islands, as of September 2016
High-tech	Binary	Main activity sector in 2016 classified by OECD/Eurostat as high or medium-high technological intensity (manufacturing), or high knowledge intensity (services). Energy sector not considered by OECD/Eurostat, classified as high-tech.
Industrial	Binary	ATECO activity sector as of September 2016: manufacturing, mining, energy
Export share	Multinomial	Value of exported goods or services as a fraction of turnover, 2016 (expectation as of September 2016)
Found survey difficult	Binary	Self-assessed difficulty of the 2016 qualitative questionnaire: 'High' or 'Excessive'
Multiple information sources	Continuous	Share of self-assessed difficulty of 2016 the qualitative questionnaire dependent on having to retrieve information from multiple sources
No outsourcing	Binary	Self-reported cybersecurity management through internal resources only
No knowledge of TTIP	Binary	Self-reported knowledge of TTIP negotiation: 'I did not know that this negotiation existed'
Share skilled	Continuous	Share of employees that are not apprentices, trainees, or manual workers over average employment, 2016
Foreign control	Binary	Self-reported locus of decision making for the firm in 2016: outside Italy

Figura 40. Definizione delle variabili utilizzate nelle regressioni dello studio di Biancotti C. [94]

I risultati dei modelli di regressione sui dati puliti sono presentati in Figura 41 e confermano le evidenze descrittive del campione: le imprese di piccole dimensioni (tra 20 e 49 dipendenti) hanno una probabilità inferiore di subire attacchi informatici e allo stesso modo le imprese del Sud. Un attacco è più probabile per le aziende che utilizzano dispositivi IoT e la motivazione potrebbe essere o la vulnerabilità specifica o il fatto che questa caratteristica rappresenta aspetti del livello tecnologico dell'impresa che non sono colti né dal settore di attività né dalla quota di manodopera qualificata sul totale della manodopera. A causa della piccola variabilità del campione, l'impatto di altre tecnologie non è statisticamente significativo.

	(i)		*(ii)*		*(iii)*	
Intercept	-0.156		-0.401	***	-0.419	***
	(0.100)		(0.123)		(0.154)	
Small	-0.109	***	-0.097	***	-0.118	***
	(0.034)		(0.037)		(0.043)	
South	-0.206	***	-0.225	***	-0.217	***
	(0.043)		(0.047)		(0.053)	
High-tech sector	0.080	**	0.040		0.034	
	(0.035)		(0.040)		(0.047)	
Industrial	-0.113	***	-0.052		-0.045	
	(0.034)		(0.039)		(0.046)	
Export share: over 2/3	0.016		0.005		0.027	
	(0.067)		(0.073)		(0.082)	
Export share: between 1/3 and 2/3	0.172	***	0.200	***	0.155	**
	(0.060)		(0.066)		(0.075)	
Found survey difficult	0.212	***	0.255	***	0.231	***
	(0.057)		(0.062)		(0.072)	
Multiple respondents involved	0.934	***	1.104	***	1.353	***
	(0.340)		(0.379)		(0.439)	
Share skilled			0.465	***	0.450	***
			(0.130)		(0.148)	
No mobile internet / cloud					-0.037	
					(0.046)	
No big data / artificial intelligence					0.020	
					(0.069)	
No internet of things					-0.115	**
					(0.059)	
N	4,254		3,657		2,854	
Percent concordant	60.1		61.0		61.9	
Percent discordant	39.0		38.5		37.7	
Percent tied	0.9		0.5		0.5	

Levels of statistical significance of coefficients : *** 1% ** 5% *10%

Figura 41. Risultati dello studio di Biancotti C. [94]

3. Dati e metodo

3.1 Il dataset

Per effettuare lo studio sulla tematica della cybersecurity in Italia sono stati utilizzati i dati raccolti da Banca d'Italia, che è la banca centrale del Paese avente diritto pubblico e regolata sia da norme europee che nazionali che garantiscono l'indipendenza da condizionamenti esterni per perseguire il mandato. Fa parte dell'Eurosistema e svolge compiti nell'interesse del settore finanziario e monetario tra cui la gestione della stabilità del sistema finanziario e dei prezzi. Tra le diverse attività svolte, si occupa di condurre indagini a campione sulle imprese italiane e ogni anno sottopone un questionario quantitativo alle imprese industriali e dei servizi non finanziari con almeno 20 dipendenti (sono escluse le attività di intermediazione finanziaria e assicurativa, la Pubblica Amministrazione, i settori della scuola e della sanità e altri servizi pubblici). In Tabella 4 viene mostrata la classificazione delle attività economiche Ateco 2007 delle imprese presenti nel campione analizzato.

	Sezione Ateco 2007	Divisione Ateco 2007	Settore di attività economica	Aggregazioni di settori utilizzate
Industria in senso stretto	C	10-12	Alimentari, bevande e tabacco	Altre manifatturiere
		13-15	Tessili, abbigliamento, pelli e calzature	Tessili, abbigliamento, pelli e calzature
		19-22	Chimica, gomma e plastica	Chimica, gomma e plastica
		23	Minerali non metalliferi	Altre manifatturiere
		24-30; 33	Metalmeccanica	Metalmeccanica
		16-18; 31-32	Altra industria manifatturiera (legno, fabbricazione pasta carta, altre industrie manifatturiere)	Altre manifatturiere
	B	05-09	Estrazioni di minerali da cave e miniere	Energetiche ed estrattive
	D	35	Fornitura di energia elettrica	Energetiche ed estrattive
	E	36-39	Fornitura di acqua	Energetiche ed estrattive
Servizi privati non finanziari	G	45-47	Commercio all'ingrosso e al dettaglio, riparazioni	Commercio, alberghi e ristorazione
	I	55-56	Attività dei servizi di alloggio e di ristorazione	
	H	49-53	Trasporti, magazzinaggio	Trasporti, magazzinaggio e comunicazioni
	J	58-63	Servizi di informazione e comunicazione	
	L, M, N	68-75; 77-82	Altri servizi a imprese e famiglie	Altri servizi a imprese e famiglie

Tabella 4. Definizione dei settori di attività economica

Il campione è selezionato in maniera casuale secondo un disegno stratificato; i risultati sono statisticamente rappresentativi per macroregione (Nord-Ovest, Nord-Est, Centro, Sud), classe dimensionale (20-49 addetti; 50-99 addetti; 100-199 addetti; 200-499 addetti; 500-999 addetti; 1000 e oltre addetti) e le aggregazioni di settore viste sopra. La valutazione viene condotta ogni anno nel periodo compreso tra febbraio e maggio, focalizzandosi sull'attività economica dell'anno precedente. Oltre a quesiti su aspetti anagrafici e strutturali, occupazione, investimenti, fatturato, risultato d'esercizio, capacità produttiva, indebitamento, i questionari contengono domande su una specifica tematica che può variare a seconda degli anni, in base alle esigenze informative del contesto in cui sono effettuate. Le

indagini studiate nel presente lavoro di ricerca sono quelle relative agli anni 2016 e 2022, che contengono una sezione dedicata al tema della cybersecurity. Nell'indagine relativa all'anno 2016 sono presenti le seguenti domande sulla cybersecurity:

Q1. *La Vostra azienda adotta le seguenti misure di sicurezza informatica (Sì/No)? (Considerate anche le attività eventualmente date in outsourcing)*

- *(i) Uso di software e/o hardware di sicurezza (es. anti-virus, firewall, ecc.)*
- *(ii) Formazione del personale all'utilizzo sicuro dei dispositivi ICT*
- *(iii) Cifratura completa o parziale dei dati*
- *(iv) Analisi e gestione delle vulnerabilità dei sistemi aziendali*

Q2. *Nel corso del 2016, approssimativamente quanto avete speso per tutelarvi dal rischio di attacchi informatici (in migliaia di euro)? Considerate i costi di tutte le attività indicate sopra e di ogni altra attività volta a prevenire gli attacchi, condotte sia da personale interno sia in outsourcing (esempi: retribuzione del personale preposto alla sicurezza e/o dei consulenti esterni; acquisto di dispositivi di sicurezza software o hardware; costi di formazione)*

Q3. *Nel corso del 2016, la Vostra impresa ha subito attacchi informatici (Sì/No)? Considerate solo quelli che hanno avuto conseguenze, anche modeste e/o di breve durata e/o facilmente reversibili, sul funzionamento dei sistemi aziendali e/o sull'integrità e la riservatezza dei dati ivi custoditi*

[Fine della sezione per le aziende che non hanno segnalato attacchi]

Q4. *Almeno uno di questi attacchi ha comportato… (Sì/No)*

- *(i) Interruzione o rallentamento dell'attività lavorativa ordinaria*
- *(ii) Ore di lavoro aggiuntive (di personale interno o consulenti esterni) per ovviare ai danni tecnici, comunicare con clienti e/o fornitori e/o azionisti in merito all'attacco, ecc*
- *(iii) Furto o distruzione di dati, inclusa la proprietà intellettuale*

Q5. *Nel corso del 2016, approssimativamente a quanto è ammontato il danno arrecatoVi da questi attacchi informatici (in migliaia di euro)? Considerate nel computo il costo delle voci sopra indicate e ogni altro costo monetario causato dagli attacchi (es. risarcimenti a clienti e fornitori, spese legali, multe di enti regolatori)*

Q6. *Avete rafforzato le Vostre misure di sicurezza dopo aver subito attacchi (Sì/No)?*

Per le domande Q2 e Q5, i partecipanti hanno avuto l'opportunità di indicare un valore puntuale in migliaia di euro oppure selezionare una delle seguenti alternative: *(i) Nessuna spesa; (ii) Meno di 10.000; (iii) Da 10.000 a 49.999; (iv) Da 50.000 a 199.999; (v) 200.000 e oltre.*

Inizialmente, le domande sono state progettate per colmare una lacuna di informazioni riguardante la frequenza degli attacchi informatici all'interno delle imprese italiane. Nello specifico contesto delle aziende in Italia, si è cercato di raccogliere dati sugli investimenti in cybersecurity effettuati, sull'entità dei danni subiti in seguito ad attacchi e delle conseguenze, e sulle misure di sicurezza informatiche al fine di avere un'idea preliminare su come le aziende affrontino il rischio informatico. La sezione dedicata alla sicurezza informatica è stata successivamente elaborata ed è stata seguita da altre sezioni che trattano di investimenti, finanziamenti, occupazione, fatturato, commercio internazionale e l'effetto dei fattori geopolitici sulle imprese, così come i pagamenti governativi alle aziende. Il campione su cui si basano i risultati relativi al 2016 presentati in questo documento includeva 4208 imprese.

Nel 2022 Banca d'Italia ha deciso di reinserire la sezione sulla cybersecurity probabilmente per fare osservazioni sull'andamento nel corso degli anni sulla situazione e valutare eventuali miglioramenti o peggioramenti del contesto. Nella relativa indagine si trovano le seguenti richieste:

Q1. *Quanto ritenete probabile che un'azienda simile alla Vostra (per dimensione e settore di attività) possa subire attacchi cibernetici?*

- *(i) Per nulla probabile*
- *(ii) Poco probabile*
- *(iii) Molto probabile*

Q2. *Nel complesso del biennio 2021-2022, approssimativamente quale spesa ha sostenuto la Vostra azienda per tutelarsi dal rischio di attacchi cibernetici?*

- *(i) Nessuna spesa*
- *(ii) Fino a 5.000€*
- *(iii) Da 5.001€ a 10.000€*
- *(iv) Da 10.001€ a 50.000€*
- *(v) Da 50.001€ a 200.000€*
- *(vi) Oltre 200.000*

Q3. *Come è variata negli ultimi 5 anni la spesa per l'acquisto di beni e servizi finalizzata ad incrementare la sicurezza informatica e prevenire incidenti IT della Vostra azienda? (Si considerino tutti gli incidenti operativi e di sicurezza sia di natura accidentale sia malevola)*

(i) Non è sostanzialmente cresciuta

(ii) È cresciuta, ma meno che raddoppiata

(iii) È più che raddoppiata

Q4. *Negli ultimi 5 anni, la Vostra azienda ha subito un danno patrimoniale a seguito di un attacco cibernetico? (Si consideri danno patrimoniale anche l'eventuale pagamento di un riscatto a fronte del ripristino dell'accesso ad alcune o tutte le funzionalità informatiche dell'azienda)*

(i) No, perché non ha subito attacchi

(ii) No, ha subito attacchi ma senza danni

(iii) Sì

Q5. *Avete una funzione aziendale (anche eventualmente in outsourcing) dedicata al governo e alla gestione della cyber-sicurezza e della continuità operativa?*

(i) No, funzione non presente

(ii) Sì, funzione completamente interna

(iii) Sì, funzione parte interna e parte in outsourcing

(iv) *Sì, funzione completamente in outsourcing*

Il campione su cui si basano i risultati relativi al 2022 presentati in questo documento includeva 4107 imprese.

È essenziale sottolineare che, affinché il questionario sia considerato attendibile secondo gli standard della Banca d'Italia, è obbligatorio fornire risposte dettagliate su determinati elementi fondamentali come occupazione, fatturato e investimenti. Le altre sezioni del questionario sono considerate opzionali. Tra queste sezioni facoltative, vi è quella dedicata alla cybersecurity. Per garantire l'integrità delle informazioni ottenute dai modelli, si è scelto di escludere dall'analisi econometrica le aziende che non hanno fornito risposte alle domande riguardanti la sicurezza informatica. Questa decisione è stata presa per proteggere la qualità e l'affidabilità dei dati estratti dall'indagine.

I risultati sono stati ottenuti attraverso l'utilizzo del software statistico Stata. Per motivi di protezione dei dati sensibili non è stato possibile ricevere direttamente i dataset da Banca d'Italia e quindi non è stato possibile eliminare eventuali missing data. Quello che è stato

possibile fare è stato inviare le richieste di elaborazione dei dati attraverso il Sistema di elaborazione a distanza (REX - Bank of Italy Remote Execution) con cui gli utenti possono condurre analisi statistiche ed econometriche senza manipolare direttamente i dati dettagliati[13]. Dopo l'autenticazione nel portale, è stato possibile caricare un programma di elaborazione scritto in uno dei linguaggi supportati e poi scaricare i risultati del processo, che devono rispettare i vincoli di rilascio[14], senza accedere direttamente ai dati di base.

3.2 Analisi descrittiva

Procediamo ora nel descrivere statisticamente come sono composti i due campioni relativi agli anni sotto analisi per avere un'idea della loro composizione e per valutare possibili relazioni presenti tra le variabili considerate successivamente nei modelli di regressione.

3.2.1 Analisi descrittiva del campione relativo all'indagine del 2016

Il campione raccolto da Banca d'Italia nel 2016 è formato da imprese distribuite abbastanza omogeneamente sul territorio italiano, con 44% delle imprese del Nord (divise tra Nord-Ovest e Nord-Est), 33% del Sud e Isole e 23% del Centro (Figura 42), ma con una prevalenza di piccole imprese per cui il 74% è composto da imprese con meno di 200 addetti (Figura 43).

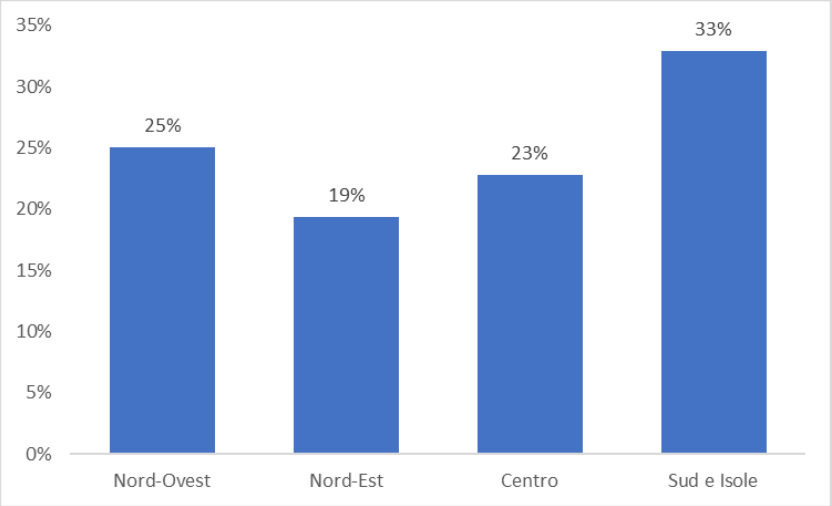

Figura 42. Distribuzione geografica delle imprese (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016])

[13] La guida all'utilizzo del Sistema REX è consultabile al seguente link: https://www.bancaditalia.it/statistiche/basi-dati/rdc/rex/user_guide_IT.pdf

[14] I vincoli di rilascio degli output sono consultabili al seguente link: https://www.bancaditalia.it/statistiche/basi-dati/rdc/rex/regole_output_IT.pdf

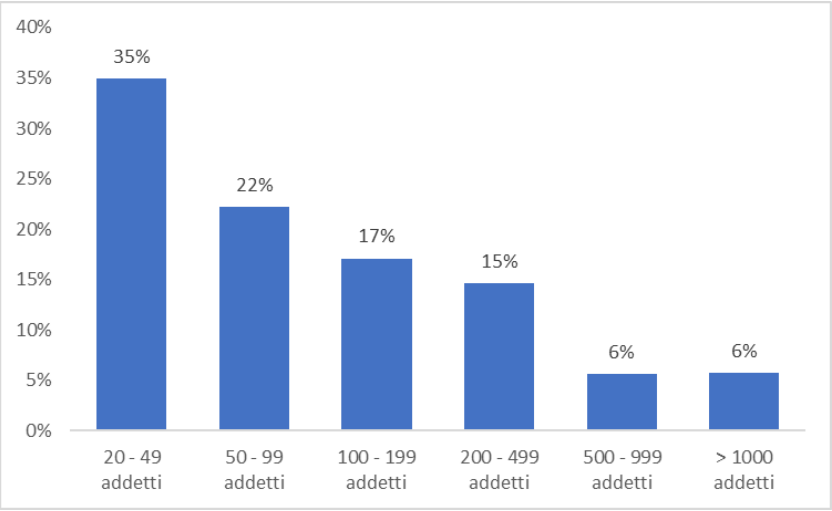

Figura 43. Dimensione delle imprese (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016])

La maggior parte delle imprese fanno parte del settore manifatturiero (67%), seguite da quelle dei servizi (29%), con una parte residua composta da quelle del settore energetico-estrattivo (6%), come si osserva in Figura 44. Inoltre, le imprese sotto analisi non sono grandi esportatrici, in quanto solo il 36% esporta oltre 1/3 del fatturato generato (Figura 45).

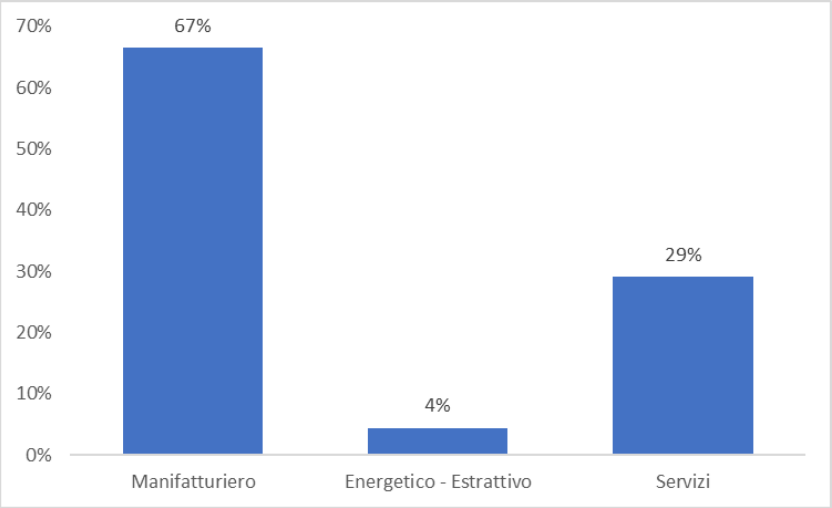

Figura 44. Settore di appartenenza delle imprese (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016])

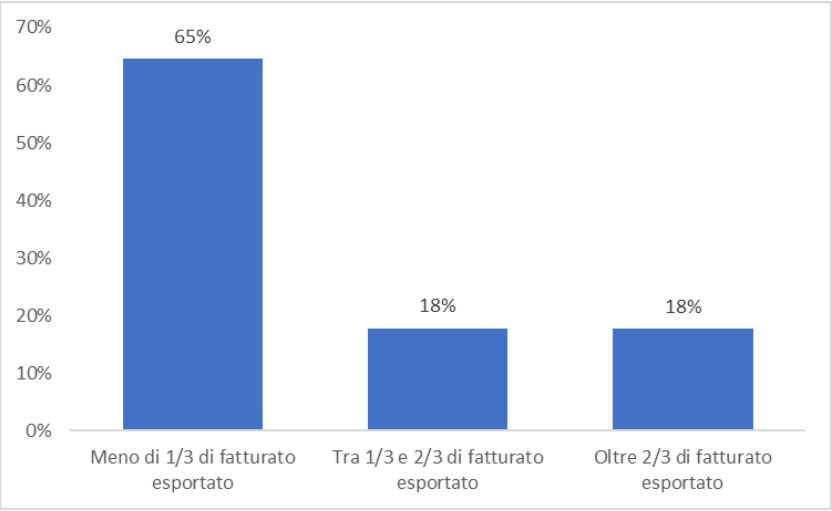

Figura 45. Quota di fatturato esportato delle imprese (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016])

Andando ad analizzare il campione in riferimento alle variabili dedicate alla sezione di cybersecurity, si osserva che, tra le imprese che hanno risposto, il 72% non ha subito alcun attacco nel corso del 2016 (Figura 46) e che il 60% ha indicato che il costo informatico dovuto agli attacchi informatici subiti nell'anno 2016 ammonta a meno di 10.000 € (Figura 47). Il danno subito medio ammonta a 38,9 mila euro (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016]). La quota di imprese che hanno indicato di non aver subito alcun attacco potrebbe essere così elevata anche per il fatto di non possedere sistemi in grado di rilevare la presenza di un attacco informatico e il 25% che ha indicato "Nessuna spesa" potrebbe essere dovuto anche alla mancanza della capacità di misurare il danno arrecato dagli attacchi.

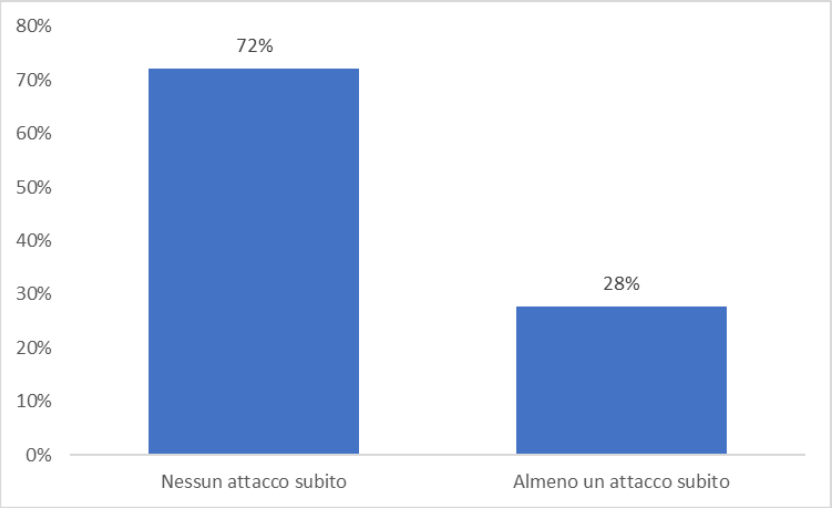

Figura 46. Percentuale di attacco subito delle imprese (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016])

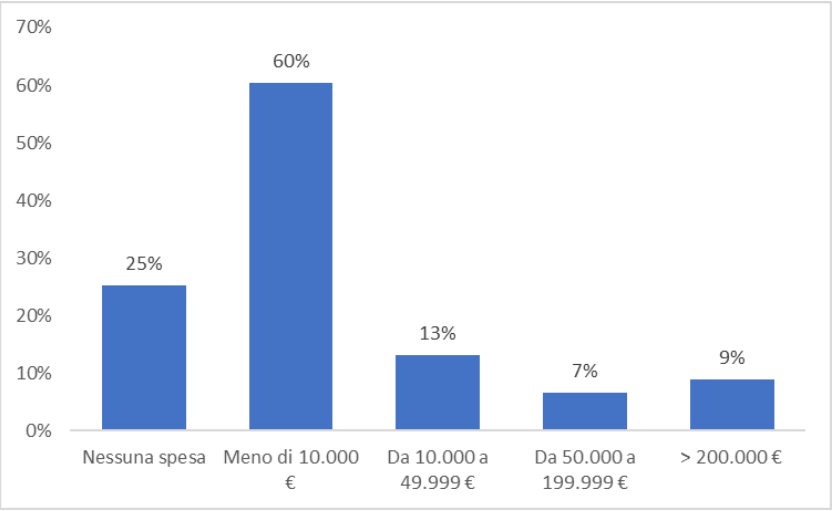

Figura 47. Costo informatico dovuto agli attacchi informatici subiti delle imprese (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016])

Abbiamo visto nel capitolo 1.3 che gli investimenti in cybersecurity sono in crescita e il fatto che solo l'8% delle imprese del campione rispondenti al quesito hanno indicato di non aver effettuato spese in sicurezza informatica nel 2016 fa intendere che anche in Italia la consapevolezza del rischio informatico era già diffusa. In media, nel corso del 2016, le imprese hanno investito 43,3 mila euro (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016]). La prevalenza di imprese che hanno investito fino a 50.000 € (Figura 48) può essere dovuta al fatto che la maggior parte del campione è composta da piccole imprese, che hanno minore disponibilità di spesa e minore valore da proteggere, e appartenenti al settore manifatturiero, caratterizzato da una presenza inferiore di dati sensibili rispetto a quello dei servizi. A parte questa ipotesi, si può osservare come l'aver subito almeno un attacco sembra essere un indicatore che spinge le imprese ad investire. Infatti, la percentuale di imprese che hanno deciso di non effettuare spese in sicurezza informatica si riduce dal 10% nel caso non abbiano subito un attacco al 3% in caso di violazione. Inoltre, si può osservare come le percentuali tendono ad aumentare nei range di investimenti maggiori, ovvero da 10.000 euro (Figura 49). Questo potrebbe significare che subire un attacco spinge il management a migliorare le difese per non subire di nuovo un attacco informatico.

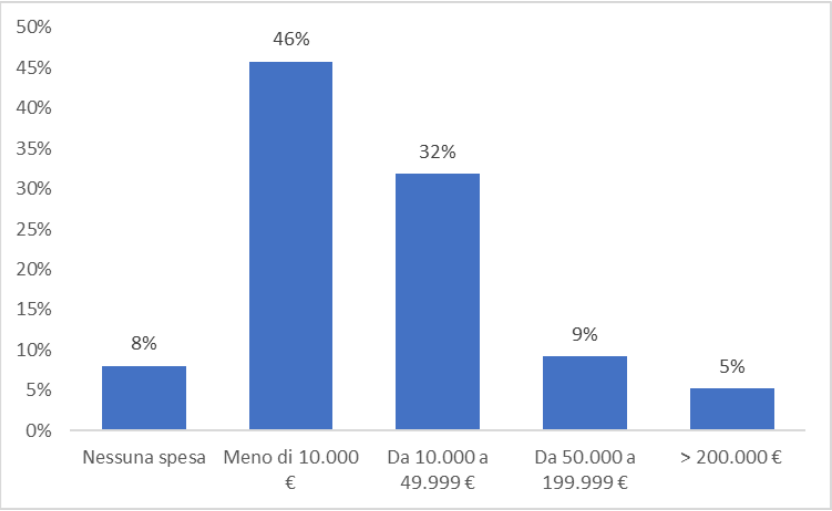

Figura 48. Investimenti in sicurezza informatica delle imprese ((Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016])

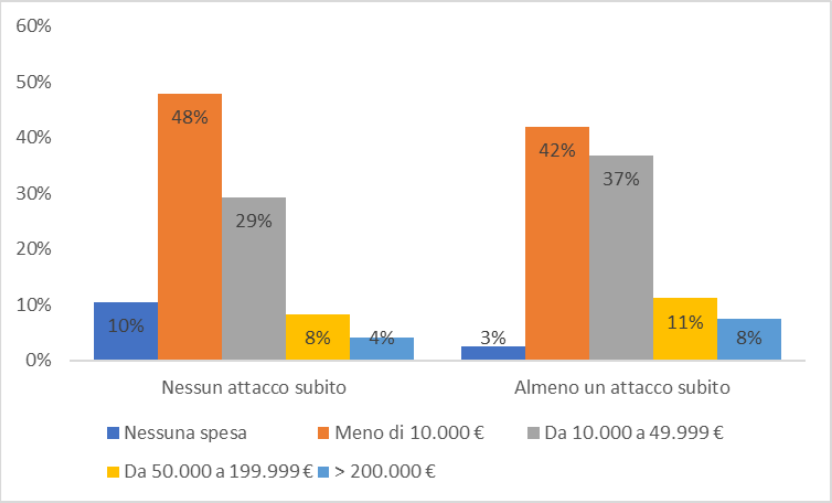

Figura 49. Investimenti in sicurezza informatica delle imprese, in relazione ad aver subito un attacco (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016])

Tra le misure di difesa adottate, l'uso di software e/o hardware di sicurezza è diffuso praticamente tra tutte le imprese rispondenti, seguita poi dalla formazione del personale all'utilizzo sicuro dei dispositivi ICT e dall'analisi e gestione delle vulnerabilità dei sistemi aziendali. Con quest'ultima si intende l'elaborare un'analisi approfondita dei sistemi operativi all'interno dell'azienda, insieme alle relative politiche di sicurezza, per individuare e correggere possibili vulnerabilità. Per ultima si trova la cifratura completa o parziale dei dati (Figura 50).

Per completezza si riportano anche le conseguenze dovute ad attacchi informatici e le principali che sono state indicate sono l'interruzione o rallentamento dell'attività lavorativa e le ore aggiuntive da dedicare alla risoluzione del problema e alla comunicazione del danno verso i principali stakeholders. Il furto o distruzione di dati, inclusa la proprietà intellettuale,

che è il danno che comporta maggiori costi e che è più difficile da quantificare, è stato segnalato nel 18% dei casi (Figura 51).

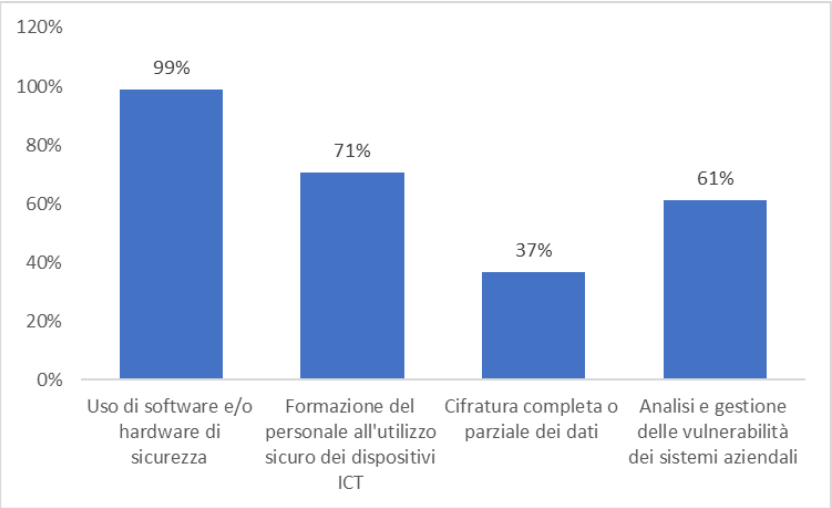

Figura 50. Misura di sicurezza informatica adottate dalle imprese (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016])

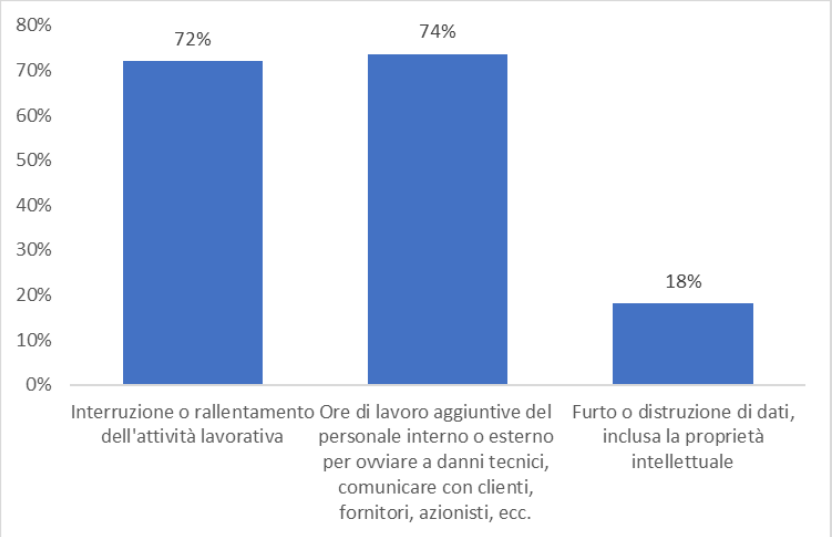

Figura 51. Conseguenze degli attacchi informatici subiti dalle imprese (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016])

Un dato che dà conforto è che l'87% delle imprese che hanno subito un attacco ha deciso di rafforzare le misure di sicurezza (Figura 52). Rafforzare le misure difensive di sicurezza informatica in seguito a un attacco cyber è di vitale importanza per diverse ragioni cruciali. Innanzitutto, un attacco cibernetico è un segnale evidente che i sistemi esistenti non sono sufficientemente protetti e che c'è urgente bisogno di miglioramenti. Aumentare la sicurezza informatica non solo protegge l'azienda da futuri attacchi, ma dimostra anche l'impegno dell'organizzazione verso la protezione dei dati sensibili dei clienti e dei dipendenti. Inoltre, rafforzare le misure difensive aiuta a ripristinare la fiducia dei clienti e degli stakeholder

nell'azienda, dimostrando che l'organizzazione è pronta a fronteggiare minacce future in modo proattivo.

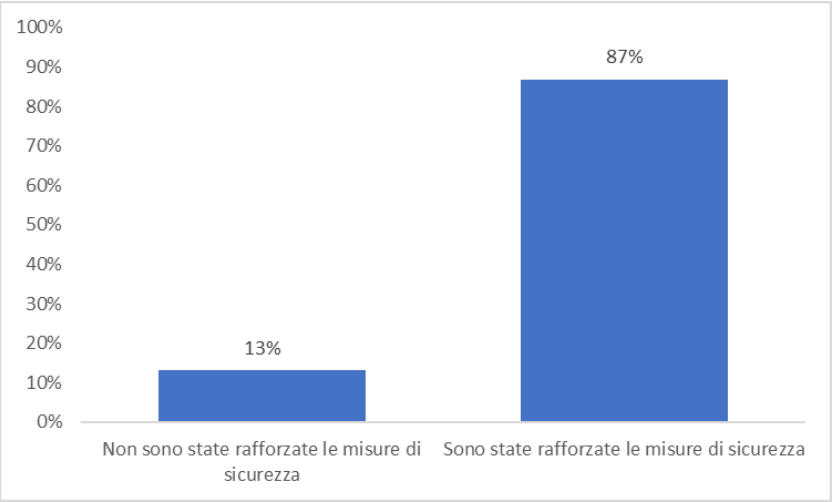

Figura 52. Percentuale di imprese che hanno rafforzato le misure di sicurezza dopo aver subito attacchi (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016])

Ma non tutte le imprese investono nello stesso modo e questa decisione può variare in base al tipo di organizzazione. Dalla Figura 53 si può dedurre come nel Sud e Isole si investa di meno: vi si trova la maggiore percentuale di imprese che non hanno effettuato alcuna spesa (14%) e la maggioranza delle rimanenti (57%) ha investito importi relativamente contenuti, inferiori a 10.000 €. Questa percentuale si riduce nel Nord-Ovest e Nord-Est a favore di un aumento di aziende che investono un budget compreso tra 10.000 e 199.000 euro. Il Centro è l'area dove si può osservare la quota maggiore di imprese che investono oltre 200.000 €. Guardando al settore in cui opera una organizzazione, in Figura 54, non sembra esserci un'influenza verso la scelta di investire più o meno: si può osservare che quasi un quinto delle imprese del settore energetico-estrattivo hanno investito più di 200.000 €.

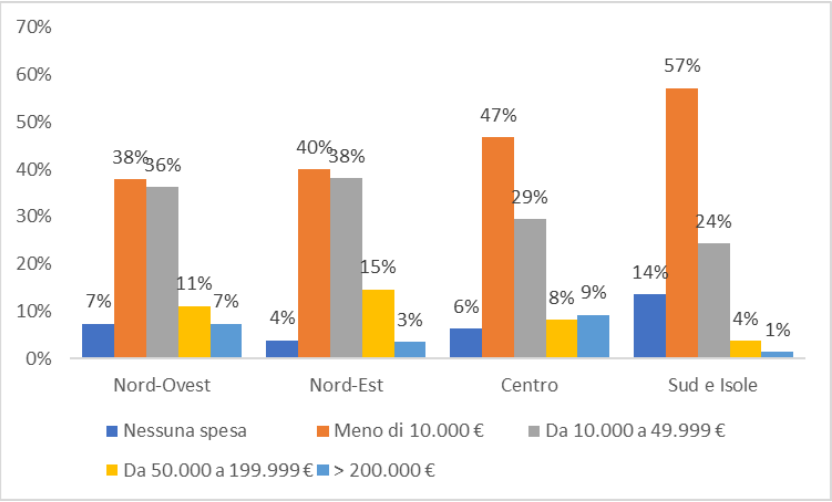

Figura 53. Investimenti in cybersecurity, per area geografica (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016])

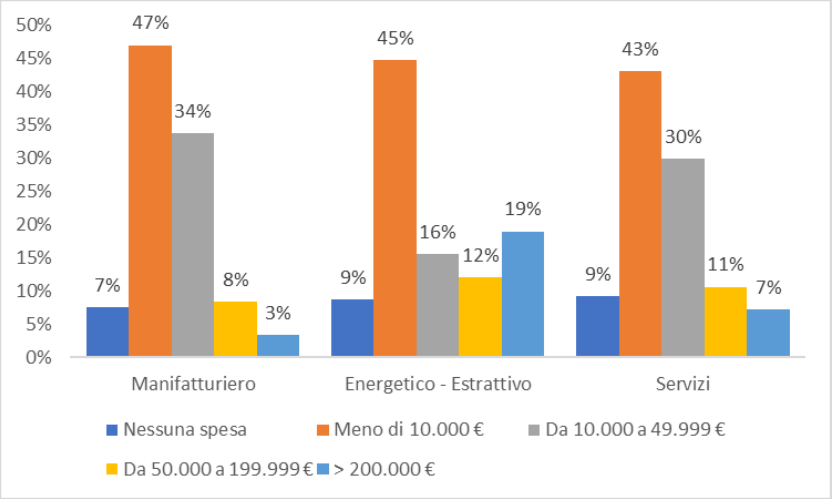

Figura 54. Investimenti in cybersecurity, per settore (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016])

Ciascuna impresa può essere o meno un obiettivo da attaccare da parte degli hacker e questo può dipendere da diversi fattori che la contraddistinguono. Se guardiamo all'area geografica, le imprese del Sud sono state meno bersagliate dalle minacce, mentre quelle del Nord hanno registrato percentuali superiore ma senza un eccessiva differenza (Figura 55). Questa differenza, invece, è più evidente se si confronta la dimensione delle organizzazioni in analisi. La prima osservazione che emerge dalla Figura 56 è che la percentuale di imprese che hanno subito almeno un attacco aumenta costantemente con l'aumentare della dimensione, e quella delle imprese che non hanno subito alcun attacco, al contrario, aumenta con il diminuire della dimensione. Tra le piccole imprese, quindi con 20-49 addetti, il 78% non ha subito alcun attacco e questa quota arriva al 58% nelle grandi imprese, intese con più di 1000 lavoratori.

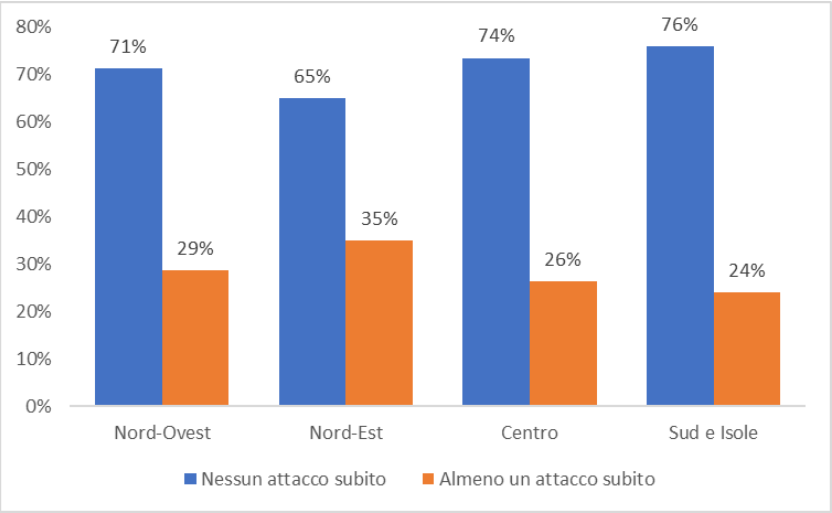

Figura 55. Percentuale di attacco subito, in base all'area (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016])

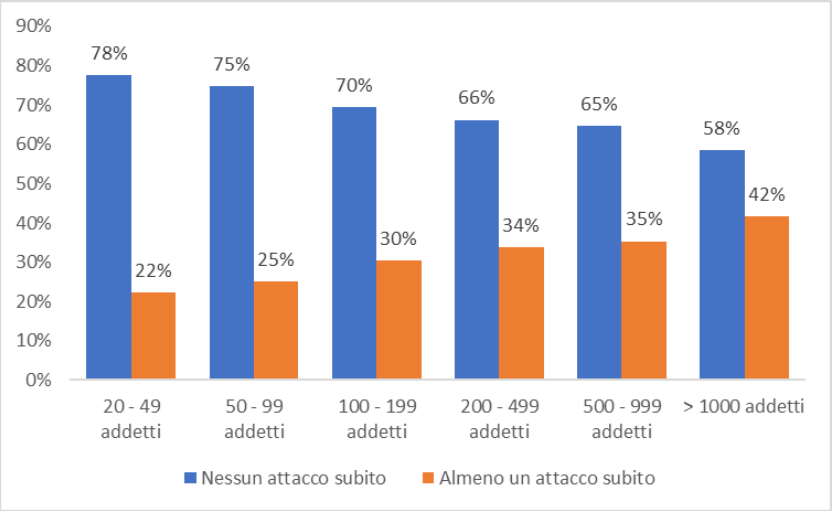

Figura 56. Percentuale di attacco subito, in base alla dimensione (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016])

Il settore in cui opera un'impresa sembra non essere un elemento che impatta la probabilità di subire una violazione informatica. Infatti, dall'analisi del dataset risulta che la percentuale di aziende che hanno subito un attacco è la stessa per i settori di appartenenza (Figura 57). La quota di fatturato esportato, invece, potrebbe influire in quanto si può notare come la segnalazione di avere subito un cyber-attacco aumenta al crescere dalla quota di fatturato esportato. Le aziende che generano oltre 2/3 del fatturato all'estero sono più inclini a essere vittime di attacchi informatici rispetto alla media (Figura 58). In questa situazione, l'esposizione svolge presumibilmente un ruolo chiave. Gli attacchi informatici, che spesso superano i confini nazionali, colpiscono principalmente le imprese che scambiano dati con partner commerciali stranieri, soprattutto in giurisdizioni considerate ad alto rischio. Queste

aziende hanno maggiori probabilità di diventare bersaglio rispetto a quelle che non interagiscono così frequentemente tramite Internet con partner esteri.

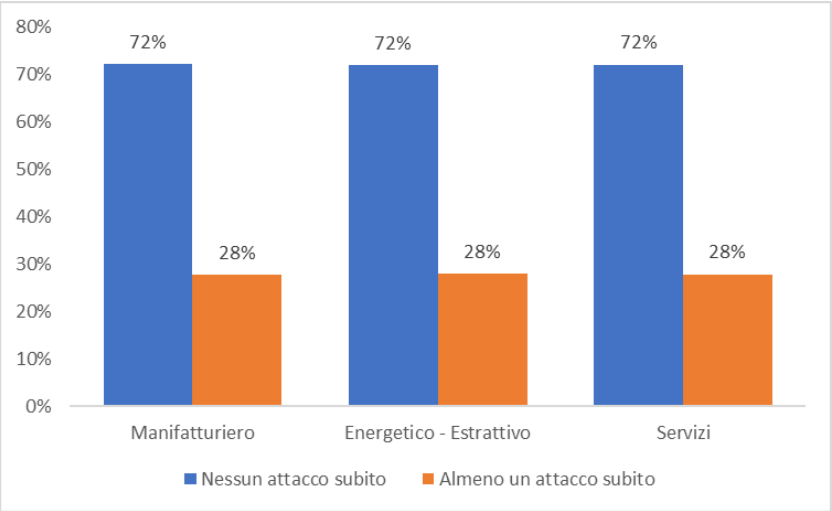

Figura 57. Percentuale di attacco subito, in base al settore (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016])

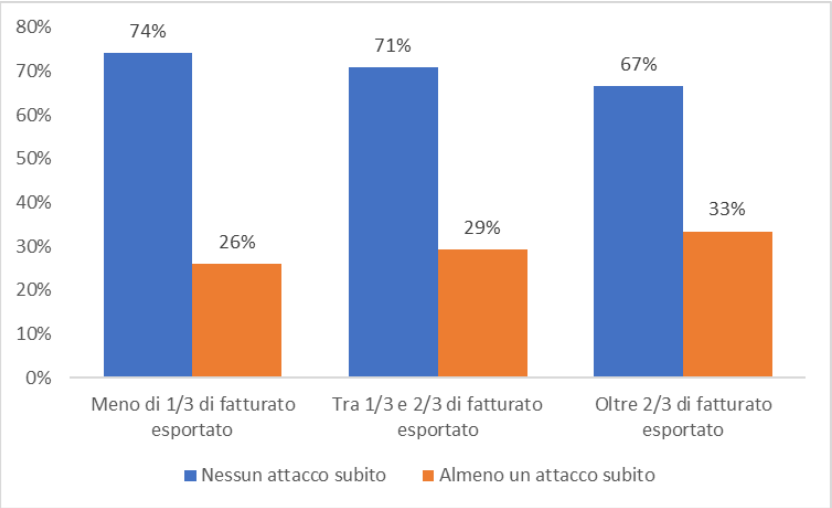

Figura 58. Percentuale di attacco subito, in base alle esportazioni (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016])

3.2.2 Analisi descrittiva del campione relativo all'indagine del 2022

Andiamo ora ad analizzare il campione raccolto da Banca d'Italia nel 2022. La distribuzione geografica è pressoché uguale a quella dell'indagine del 2016, con 44% delle imprese del Nord (divise tra Nord-Ovest e Nord-Est), 34% del Sud e Isole e 22% del Centro (Figura 59), raccogliendo nuovamente una prevalenza di piccole imprese per cui il 72% è composto da imprese con meno di 200 addetti (Figura 60).

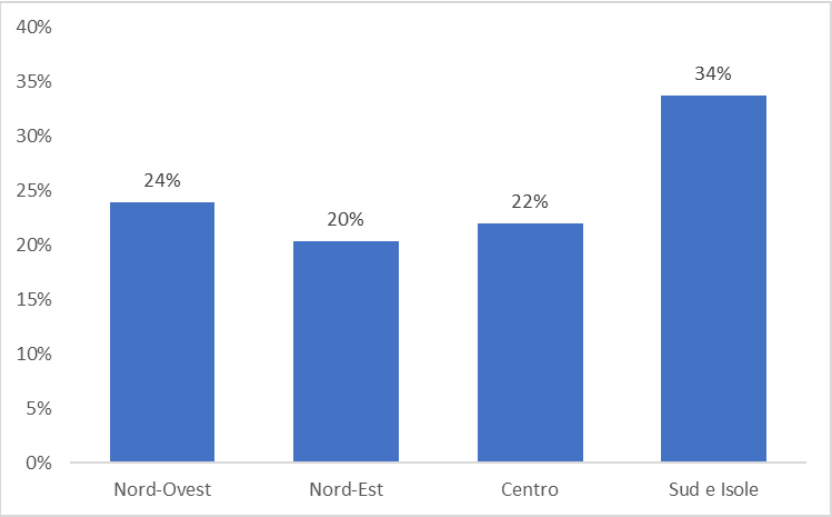

Figura 59. Distribuzione geografica delle imprese (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

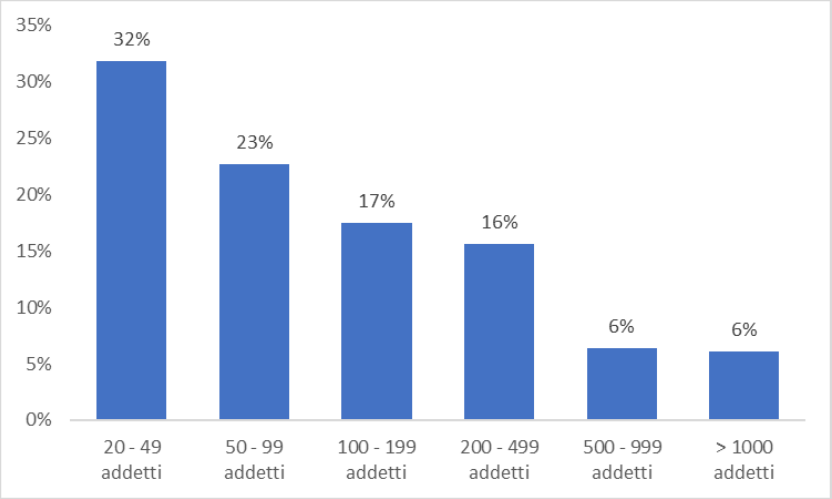

Figura 60. Dimensioni delle imprese (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

Anche per l'anno 2022 la maggioranza delle aziende coinvolte nell'indagine proviene dal settore manifatturiero (63%), seguite da quelle del settore dei servizi (32%). Un numero esiguo di partecipanti appartiene al settore energetico-estrattivo (5%), come illustrato nella Figura 61. È interessante notare che le aziende sottoposte all'analisi non sono prevalentemente orientate all'esportazione e la percentuale è ancor più ridotta rispetto al 2016: solo il 33% di esse esporta oltre un terzo del proprio fatturato, come indicato in Figura 62.

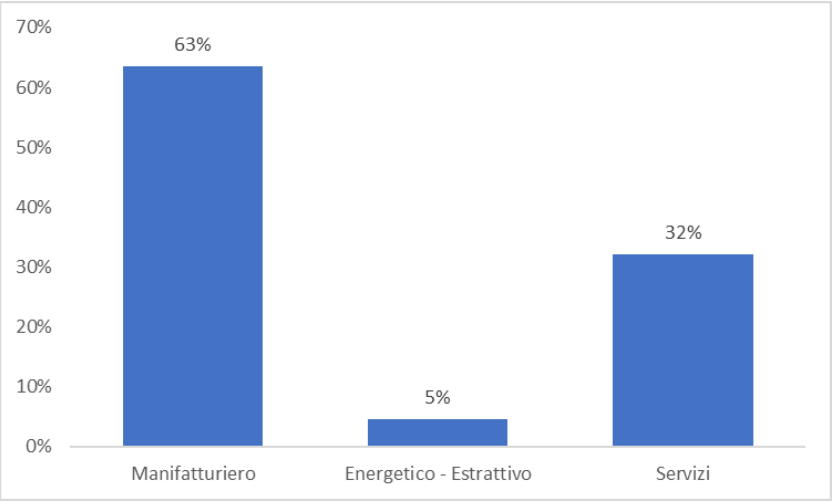

Figura 61. Settori di appartenenza delle imprese (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

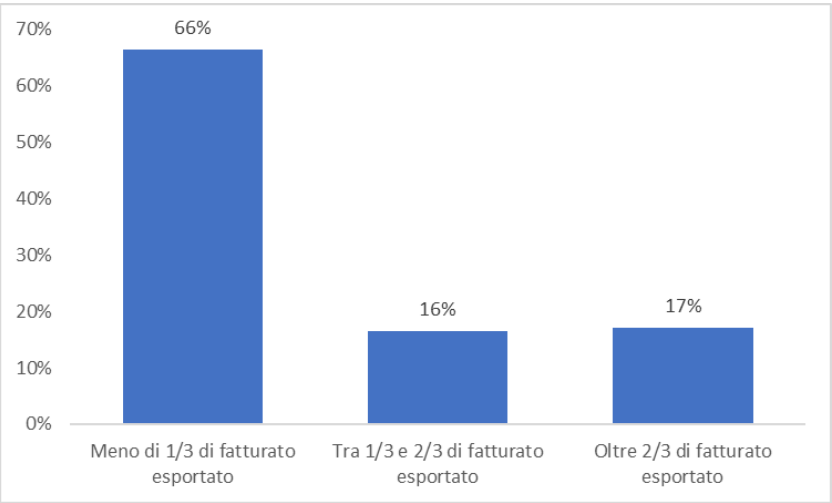

Figura 62. Quota di fatturato esportato delle imprese (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

È interessante valutare se la tendenza ad investire sia effettivamente migliorata, peggiorata o rimasta invariata. Il dato che salta subito all'occhio è che la percentuale di imprese che non hanno effettuato investimenti in cybersecurity è aumentata al 19%, rispetto all'8% del campione del 2016. Si può osservare che anche le percentuali di rispondenti sulla spesa fino ai 10.000 € sia aumentata dal 46% al 49%, mentre sono diminuite quelle relative agli investimenti fino a 50.000 €, tra 50.000 e 200.000 € e oltre (Figura 63). In generale, quindi, si osserva che la percentuale di imprese che hanno investito è diminuita ma è diminuita anche la tendenza ad investire somme maggiori.

Il motivo per cui quasi una impresa su cinque non ha investito in cybersicurezza può essere ritrovato nella poca consapevolezza sulla probabilità di subire un attacco. Infatti, il 61% delle imprese ritiene poco probabile che, viste le dimensioni e il settore, possa subire un attacco

cibernetico e il 10% addirittura considera questa probabilità nulla (Figura 64). La consapevolezza della probabilità di subire un attacco cibernetico è fondamentale per le aziende in questa era digitale in cui le minacce informatiche sono sempre più sofisticate e pervasive. Riconoscere che nessuna azienda è immune agli attacchi informatici è il primo passo per sviluppare una strategia di sicurezza robusta.

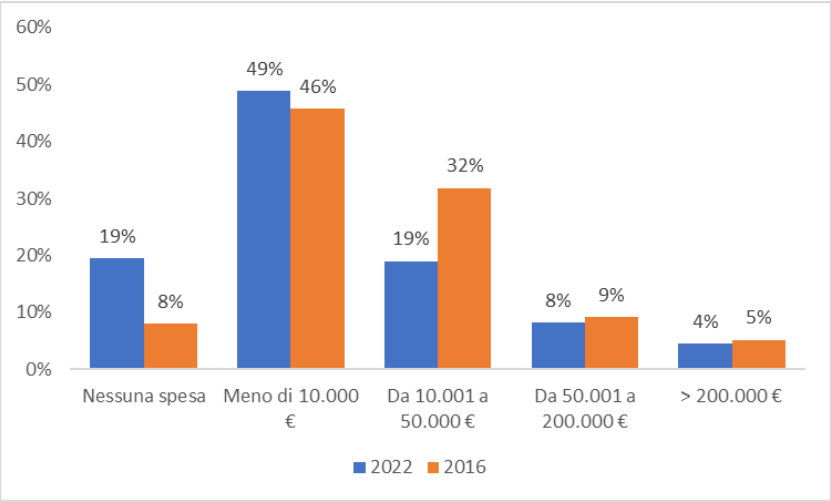

Figura 63. Investimenti in sicurezza informatica 2022 vs 2016 (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016, 2022])

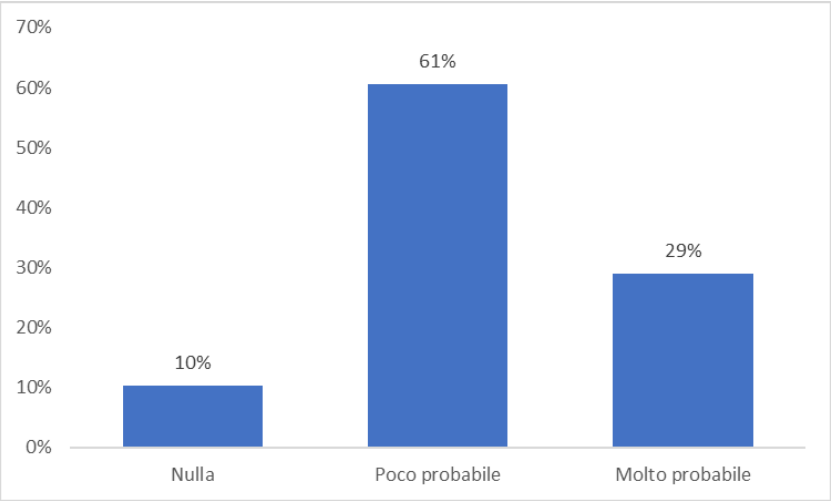

Figura 64. Consapevolezza sulla probabilità di subire un attacco (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

Infatti, vista la poca consapevolezza del poter subire un attacco, risulta che negli ultimi 5 anni la variazione della spesa in sicurezza informatica non è variata nel 44% dei casi (Figura 65). Questo dato non è in linea con le recenti tendenze sugli attacchi informatici in costante aumento nel nostro Paese, analizzate nel capitolo 1.2. Oltre ad aumentare il numero di attacchi cyber, stanno migliorando anche le capacità e le tecniche usata dagli hacker per danneggiare un'organizzazione, ed è quindi necessario che le aziende si muovano per

contrastare le minacce cercando di aumentare gli investimenti in cybersecurity negli anni in modo da stare al passo con il contesto che le circonda.

In aggiunta, è interessante notare che anche nel 2022 circa il 70% delle aziende coinvolte nell'analisi non ha riportato alcuna violazione informatica, come evidenziato nella Figura 66. Il dato che riporta il 24% delle aziende che hanno subito un attacco ma non hanno risentito di un danno patrimoniale è da prendere con il beneficio del dubbio perché potrebbero non avere le competenze per misurare il relativo costo dell'attacco.

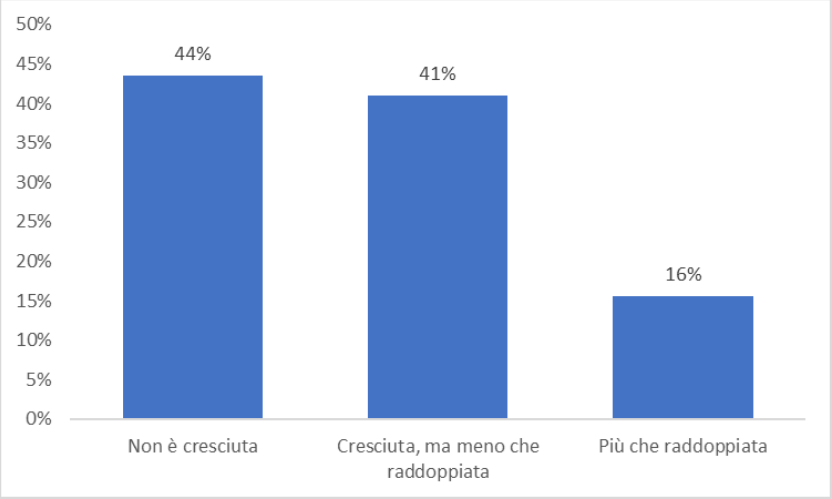

Figura 65. Variazione negli ultimi 5 anni della spesa in sicurezza informatica (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

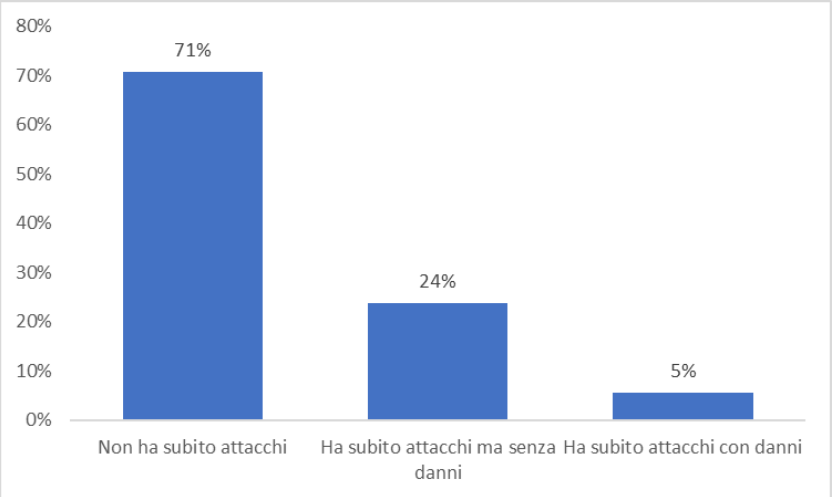

Figura 66. Danno patrimoniale a seguito di un attacco cibernetico (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

In aggiunta, può essere curioso analizzare come la funzione aziendale dedicata al governo e alla gestione della cyber-sicurezza e della continuità operativa sia internalizzata o esternalizzata. È emerso che il 31% delle imprese non dispone di una funzione dedicata a queste attività, nonostante sia importante avere un dipartimento aziendale per proteggere

l'azienda da attacchi informatici, garantendo la sicurezza dei dati sensibili e assicurando la continuità delle operazioni, compresa la ripresa delle attività in caso di incidenti. Nel 27% dei casi questa funzione aziendale è completamente internalizzata, offrendo numerosi vantaggi, tra cui una profonda comprensione del contesto aziendale, la capacità di rispondere prontamente agli incidenti e l'abilità di sviluppare soluzioni personalizzate per affrontare le minacce specifiche dell'organizzazione. La preferenza di affidare questi compiti interamente in outsourcing è diffusa nel 16% delle imprese: l'esternalizzazione a fornitori specializzati offre un accesso immediato a esperienze e risorse avanzate, permettendo all'azienda di concentrarsi sul nucleo del proprio business, ma comporta il rischio di perdere un controllo diretto e richiede una gestione attenta del fornitore per garantire sicurezza e conformità. L'internalizzazione della cybersecurity offre maggiore controllo e flessibilità, ma può richiedere investimenti sostanziali in formazione e tecnologie, oltre a mettere pressione sulla disponibilità di personale altamente qualificato, che sono risorse che un'impresa potrebbe non possedere. Infine, il 26% delle aziende rispondenti ha indicato di scegliere un'alternativa ibrida, disponendo di funzioni aziendali dedicate alla cybersecurity sia interne che esterne all'organizzazione (Figura 67).

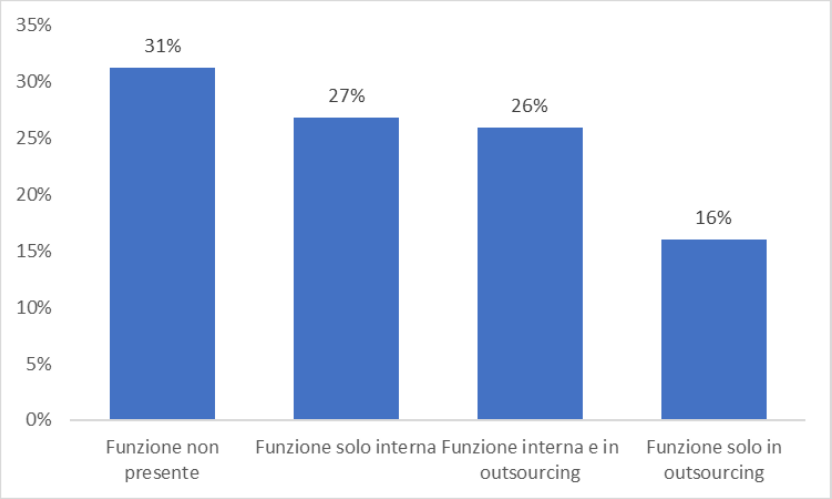

Figura 67. Internalizzazione o outsourcing della funzione aziendale dedicata alla gestione della cyber-sicurezza (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

È interessante osservare la distribuzione delle risposte in merito agli investimenti in cybersecurity effettuati nel biennio 2021-2022 in base all'area geografica, la dimensione e il settore dell'impresa. I dati fanno emergere come il Sud investe di meno con 25% delle imprese che non hanno effettuato spese e 55% hanno investito fino a 10.000 euro, mentre l'importo degli investimenti aumenta nel Centro e poi ancora nel Nord (Figura 68). Anche in questo caso si può notare come il budget destinato agli investimenti in cybersecurity

aumenti con la dimensione dell'impresa (Figura 69). Un dato importante emerso è che nelle organizzazioni grandi (con 1.000 addetti e oltre) il 42% ha investito una spesa maggiore di 200.000 euro. Guardando la Figura 70, il settore non ha indicato una particolare evidenza di settori in cui si investe maggiormente: possiamo osservare solamente che il settore che ha la maggiore quota di imprese che hanno investito meno di 5.000 euro è quello energetico-estrattivo, mentre quello con quella di imprese che hanno speso da 50.000 a 200.000 è quello dei servizi non finanziari.

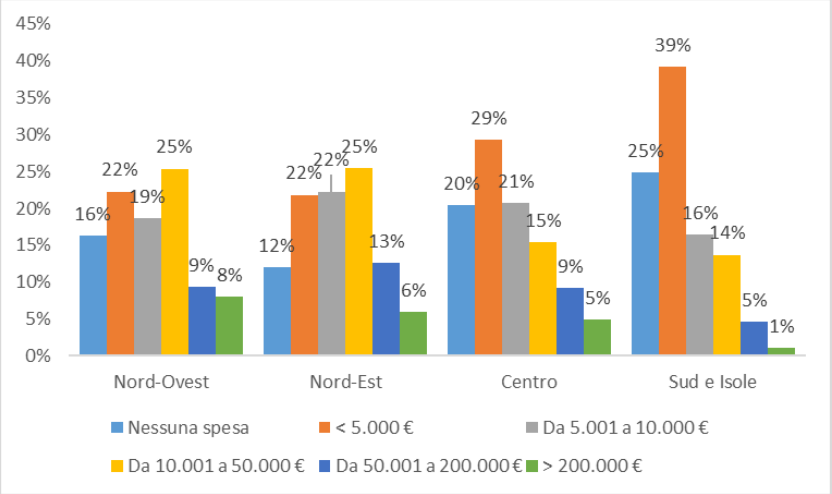

Figura 68. Investimenti in cybersecurity nel biennio 2021-2022, per area geografica (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

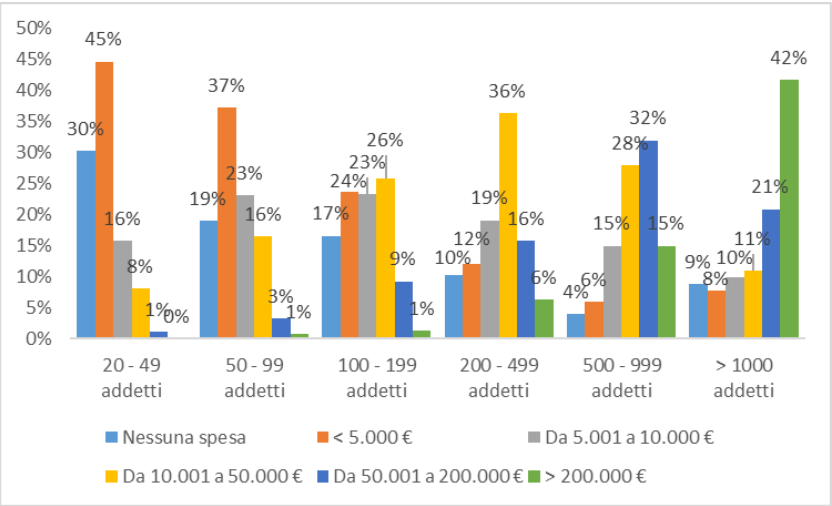

Figura 69. Investimenti in cybersecurity nel biennio 2021-2022, per dimensione (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

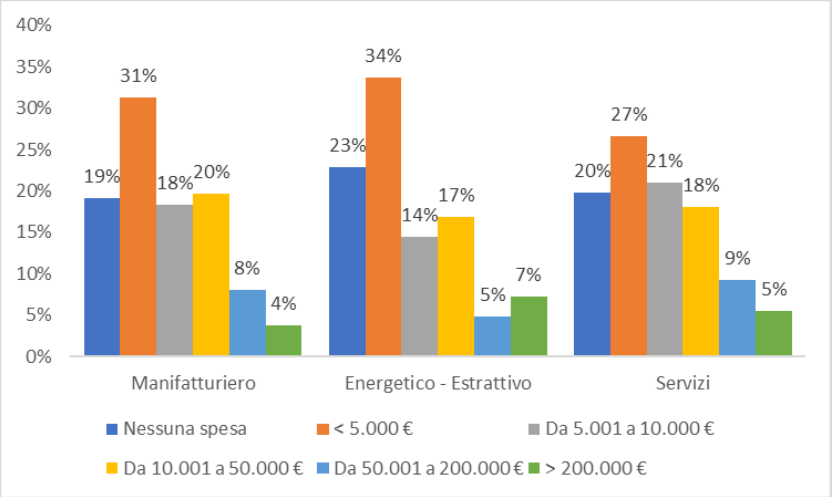

Figura 70. Investimenti in cybersecurity nel biennio 2021-2022, per settore (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

Il fatto di aver subito un attacco negli anni precedenti può essere un indicatore valido per spingere un'impresa a dedicare parte del budget disponibile agli investimenti a quelli relativi al miglioramento della cybersecurity, come si può vedere in Figura 71. Le percentuali di imprese che hanno effettuato nessuna spesa o inferiore a 5.000 euro diminuiscono nel caso di attacco subito, mentre aumentano negli altri intervalli di investimento. Inoltre, aver subito un danno patrimoniale in seguito all'attacco sembra vincolare la capacità di spesa delle imprese, che spendono meno rispetto al caso di aver subito attacchi ma senza danni economici.

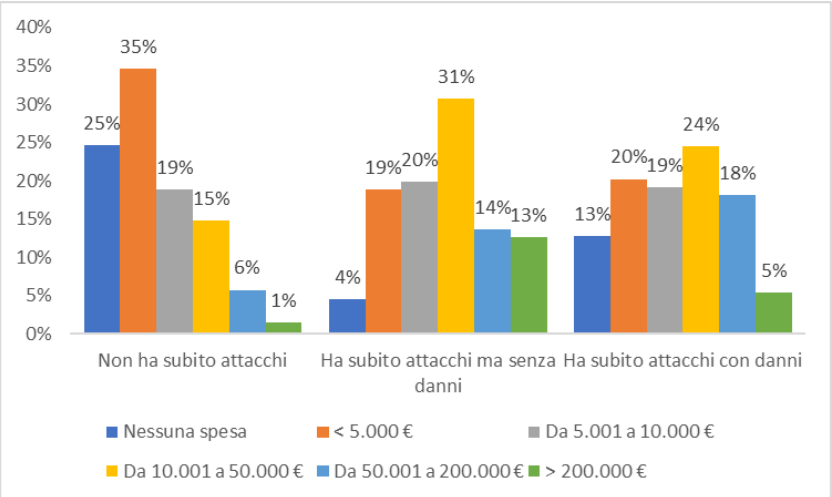

Figura 71. Investimenti in cybersecurity nel biennio 2021-2022, per attacco e danno subiti nei cinque anni precedenti (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

Oltre ad osservare gli investimenti avvenuti nel biennio 2021-2022, può essere indicativo valutare come la spesa in sicurezza informatica sia variata negli ultimi cinque anni. L'ipotesi per cui la dimensione influenza la scelta delle imprese ad investire è ripetuta anche

guardando a questo periodo di tempo. Infatti, si osserva in Figura 72 che la maggior parte di imprese in cui la spesa è più che raddoppiata sono quelle con oltre 1.000 addetti, mentre quelle in cui la spesa non è cresciuta sono di piccole dimensioni. Ma, nuovamente, il settore non è un indicatore sulla scelta di investire (Figura 73).

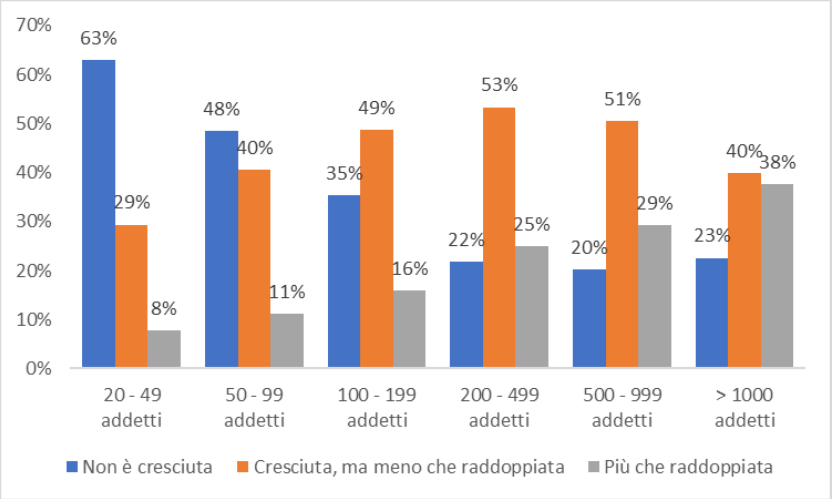

Figura 72. Variazione spesa in cybersecurity negli ultimi cinque anni, per dimensione (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

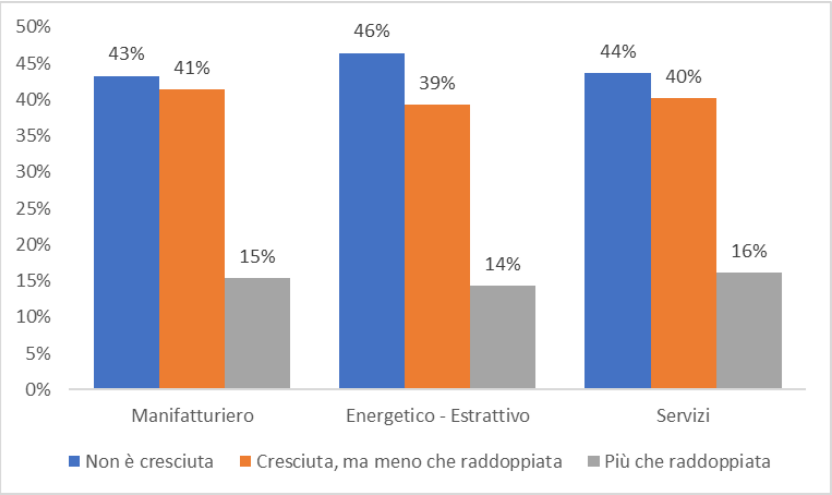

Figura 73. Variazione spesa in cybersecurity negli ultimi cinque anni, per settore (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

Il fatto che le imprese abbiano subito un attacco e/o un relativo danno patrimoniale negli scorsi anni sembra determinare una variazione di spesa in cybersecurity. infatti, come si vede in Figura 74, nel caso di imprese che non hanno subito attacco non vi è stata variazione negli investimenti. Le organizzazioni che sono state vittime di attacchi hanno incrementato il budget speso nella sicurezza informatica e, in quelle che hanno registrato anche un danno

patrimoniale, si osserva una maggiore percentuale di raddoppio dell'investimento effettuato nel corso degli ultimi cinque anni.

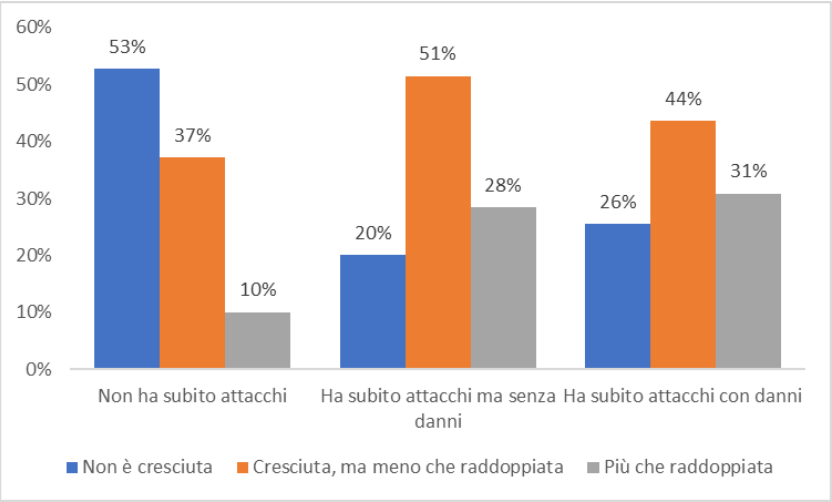

Figura 74. Variazione di spesa negli ultimi cinque anni, per attacco e/o danno patrimoniale (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

In aggiunta, è utile dare una panoramica sulle caratteristiche delle imprese che hanno subito un danno patrimoniale in seguito ad un attacco cibernetico negli ultimi cinque anni. Come era stato osservato nel campione del 2016, la dimensione può essere un fattore che influenza la probabilità di subire un attacco per cui imprese di grandi dimensioni sono bersagli più appetibili per i malintenzionati e sono più propense a registrare danni economici rilevanti; al contrario, realtà di dimensioni ridotte vengono considerate obiettivi di minore valore (Figura 75). Il settore non è influente sulla scelta degli attaccanti sul violare o meno la difesa di un'organizzazione, come mostrano le percentuali in Figura 76, e il Nord è maggiormente coinvolto in attacchi cibernetici rispetto al Centro e Sud del Paese (Figura 77). Per quanto riguarda le esportazioni, nel dataset del 2022 è meno evidente rispetto al 2016 la preferenza di bersagliare imprese esportatrici ma comunque si riscontra che la percentuale di attacco subito aumenta quando la quota di fatturato esportato supera 1/3 di quello generato (Figura 78).

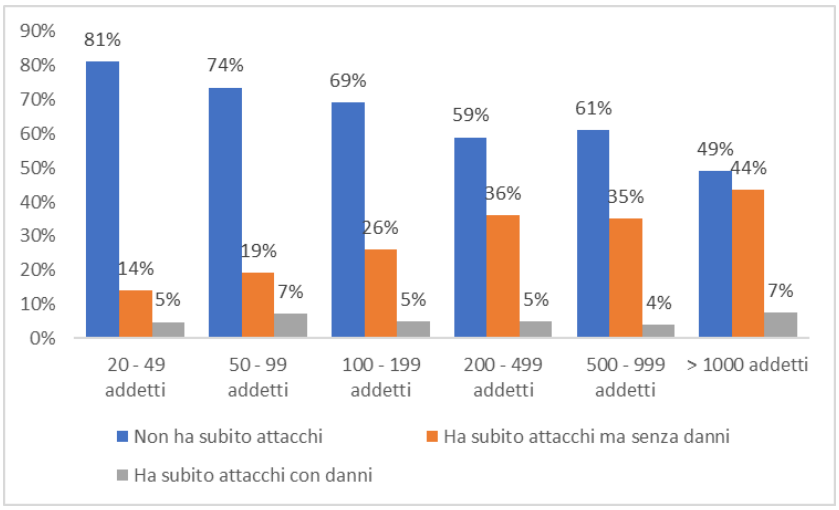

Figura 75. Danno patrimoniale dovuto ad attacchi cibernetici negli ultimi cinque anni, per dimensione (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

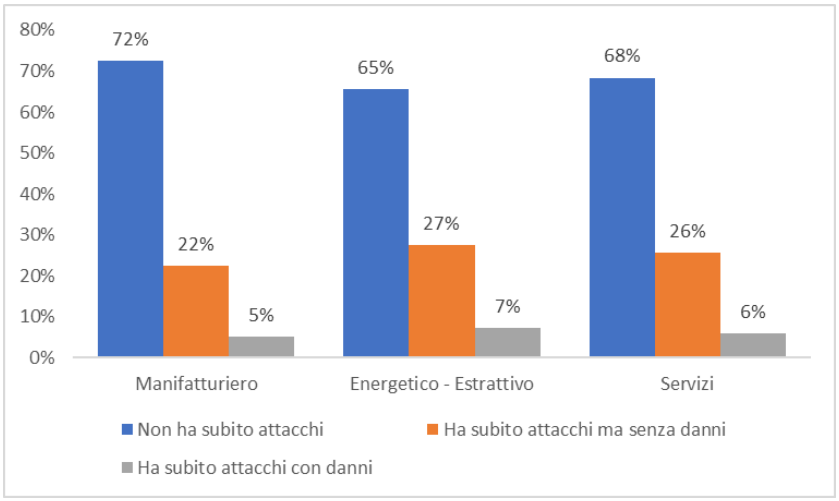

Figura 76. Danno patrimoniale dovuto ad attacchi cibernetici negli ultimi cinque anni, per settore (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

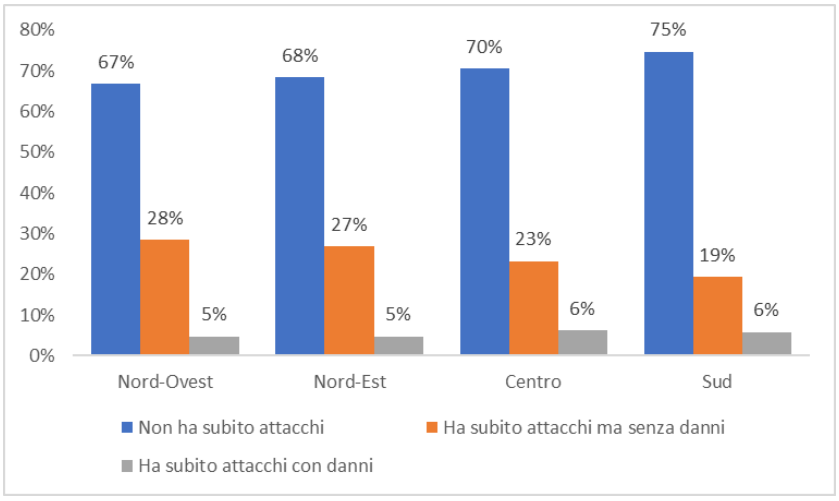

Figura 77. Danno patrimoniale dovuto ad attacchi cibernetici negli ultimi cinque anni, per area (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

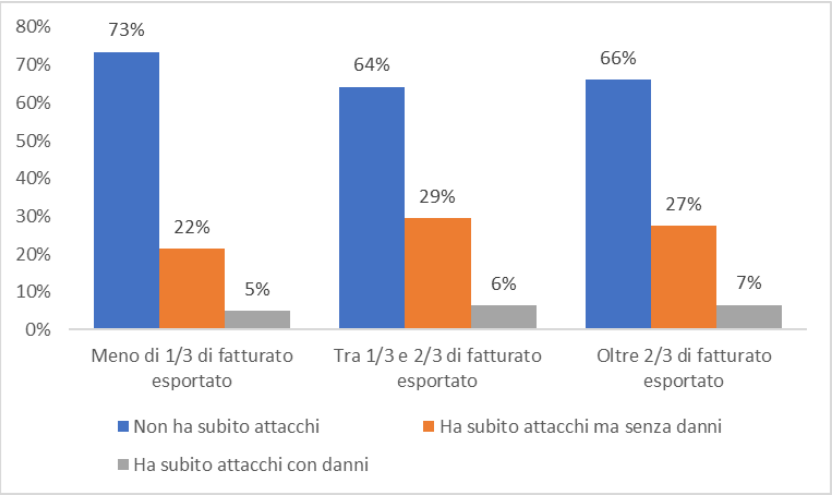

Figura 78. Danno patrimoniale dovuto ad attacchi cibernetici negli ultimi cinque anni, per quota di esportazione (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

Provando a cercare di identificare le imprese più consapevoli di poter subire un attacco cibernetico, si osserva come più del 30% delle imprese del Nord considerino molto probabile che siano un obiettivo degli attaccanti hacker, mentre quelle del Sud e Isole risultano meno coscienti di tale minaccia poiché solo il 25% ritiene altamente probabile una violazione e il 15% non vede alcuna probabilità del verificarsi di un tale evento (Figura 79). Le imprese dei servizi sembrano essere al corrente di poter subire con maggiore probabilità un attacco cyber (Figura 80), visto anche l'elevato numero di dati sensibili che possiedono e che utilizzano quotidianamente.

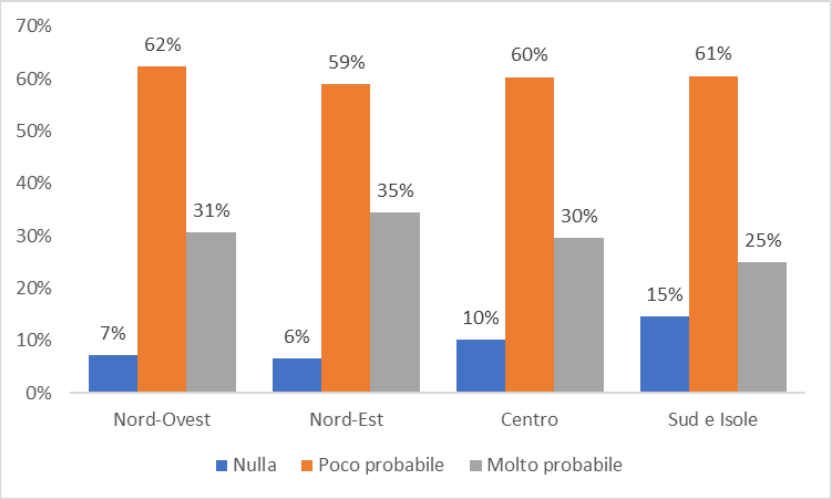

Figura 79. Consapevolezza della probabilità di poter subire un attacco cibernetico, per area geografica (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

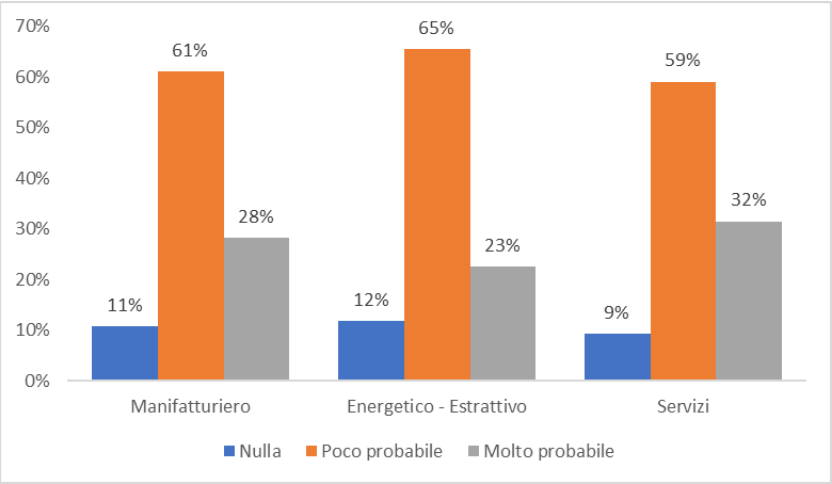

Figura 80. Consapevolezza di poter subire un attacco cibernetico, per settore (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

La quota di esportazione, come abbiamo anche visto nel caso della scelta di investire e sugli attacchi subiti, gioca un ruolo anche nella consapevolezza cyber. Le imprese esportatrici di oltre 2/3 del fatturato si ritengono più favorevoli ad essere bersagli degli hacker. La percentuale delle imprese che hanno risposto "Molto probabile" sulla possibilità di subire un attacco aumenta all'aumentare del fatturato esportato, come si osserva in Figura 81.

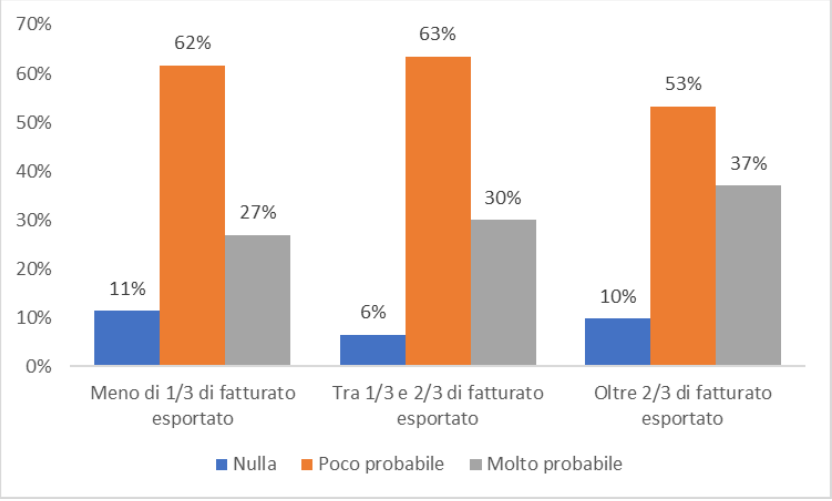

Figura 81. Consapevolezza di poter subire un attacco cibernetico, per quota di fatturato esportato (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

3.3 Il metodo OLS

3.3.1 Regressione lineare

Per poter ottenere risposta ai nostri quesiti viene utilizzato il modello econometrico OLS (*Ordinary Least Square*), ovvero il metodo dei minimi quadrati ordinari che attribuisce ai parametri della relazione quei valori che riducono al minimo la somma dei quadrati delle differenze tra le osservazioni effettive della variabile dipendente e i valori predetti dalla retta

di regressione stimata. Queste discrepanze, spesso chiamate "residui", rappresentano le distanze tra le osservazioni reali e la retta di regressione stimata. Il modello di regressione lineare semplice ha la seguente relazione generica:

$$Y_i = \beta_0 + \beta_1 X_i + u_i$$

in cui si hanno n osservazioni (X_i, Y_i) con $i = 1, \dots, n$.

- X è la variabile indipendente o regressore
- Y è la variabile dipendente
- β_0 = intercetta della retta di regressione
- β_1 = pendenza (o coefficiente angolare) della retta di regressione
- u_i = errore (o residuo) di regressione

La pendenza della retta di regressione indica l'effetto atteso sulla variabile Y di una variazione unitaria della variabile X. Il residuo u_i è costituito dai fattori omessi, ovvero non osservabili oppure omessi dall'analisi per scelta, che sono differenti dalla variabile X ma che influenzano Y.

Lo stimatore OLS di β_0 e β_1 è dato dalla soluzione del seguente problema di minimizzazione:

$$min_{b_0,b_1} \sum_{i=1}^{n} [Y_i - (b_0 + b_1 X_i)]^2$$

Infatti, questo stimatore ha l'obiettivo di minimizzare la somma dei quadrati delle differenze tra i valori reali osservati di Y_i e i valori predetti dalla retta di regressione stimata $b_0 + b_1 X_i$.

Il problema di minimizzazione presentato può essere risolto attraverso il calcolo differenziale, per cui gli stimatori OLS della pendenza β_1 e dell'intercetta β_0 sono:

$$\widehat{\beta_1} = \frac{\sum_{i=1}^{n}(X_i - \bar{X})(Y_i - \bar{Y})}{\sum_{i=1}^{n}(X_i - \bar{X})^2} = \frac{s_{XY}}{s_X^2}$$

$$\widehat{\beta_0} = \bar{Y} - \widehat{\beta_1}\bar{X}$$

Dopo aver determinato le stime dei parametri, i valori predetti di Y_i e dei residui u_i sono:

$$\widehat{Y_\iota} = \widehat{\beta_0} + \widehat{\beta_1} X_i$$

$$\widehat{u_\iota} = Y_i - \widehat{Y_\iota}$$

Per misurare la bontà dell'adattamento della regressione ai dati si possono usare diversi indicatori, tra cui:

$$R^2 = \frac{ESS}{TSS} = \frac{\sum_{i=1}^{n}\left(\widehat{Y_\iota} - \bar{\widehat{Y}_\iota}\right)^2}{\sum_{i=1}^{n}(Y_i - \bar{Y})^2}$$

$$RMSE = \sqrt{\frac{1}{n}\sum_{I=1}^{n} \widehat{u_i}^2}$$

La misura dell'R^2 indica la percentuale di varianza campionaria di Y_i spiegata dalla regressione e varia tra zero, che indica nessun adattamento, e uno, che rappresenta perfetto adattamento. Nello specifico ESS (*Explained Sum of Squares*) è la frazione di varianza spiegata e TSS (*Total Sum of Squares*) è la varianza totale. Per questo, $R^2 = 1$ rappresenta perfetto adattamento della regressione ai dati, per cui la frazione di varianza spiegata coincide con la varianza totale. L'$RMSE$ (Root Mean Standard Error) misura la dimensione del residuo di regressione nell'unità di misura di Y.

Il metodo OLS si basa sulle cosiddette assunzioni dei minimi quadrati, che devono valere per poter ottenere degli stimatori corretti dei parametri veri:

1. La distribuzione di u condizionata a X ha media nulla, cioè $E(u|X = x) = 0$. Ovvero, per ogni dato valore di X, la media di u è zero. Questo comporta che $\widehat{\beta_1}$ sia non distorto.
2. $(X_i, Y_i), i = 1, \dots, n$, sono indipendenti e identicamente distribuiti. Per rendere vera questa ipotesi la raccolta dei dati deve avvenire mediante campionamento casuale semplice.
3. Gli outlier in X e/o Y sono rari, ovvero hanno momenti quarti finiti ($E(X^4) < \infty, E(Y^4) < \infty$).

Se valgono le ipotesi dei minimi quadrati, in grandi campioni, la distribuzione di $\widehat{\beta_1}$ è normale, per cui $E(\widehat{\beta_1}) = \beta_1$ e per calcolare l'errore standard, ovvero l'incertezza campionaria, si utilizza la seguente formula:

$$var(\widehat{\beta_1}) = \frac{1}{n} \times \frac{var[(X_i - \bar{X})u_i]}{[var(X_i)]^2}$$

Si può osservare che $var(\widehat{\beta_1})$ è inversamente proporzionale a n ed è inversamente proporzionale alla varianza di X, per cui più è grande la varianza di X, più è piccola la varianza di $\widehat{\beta_1}$.

Dopo aver trovato gli stimatori, si vuole verificare che siano significativi sui dati del campione. L'obiettivo è verificare che l'ipotesi nulla H_0 sia corretta oppure no. L'impostazione generale di ipotesi nulla e ipotesi alternativa bilaterale è quella che segue:

$$H_0: \beta_1 = \beta_{1,0} \text{ vs. } H_1: \beta_1 \neq \beta_{1,0}$$

in cui di solito $\beta_{1,0} = 0$, per cui $\beta_1 = 0$ indica che non c'è alcun impatto sulla variabile dipendente.

Per effettuare la verifica si procede costruendo la statistica t e calcolando il $p - value$. In generale:

$$t = \frac{stimatore - valore\ ipotizzato}{errore\ standard\ dello\ stimatore}$$

e, quindi, per verificare β_1:

$$t = \frac{\beta_1 - \beta_{1,0}}{SE(\widehat{\beta_1})}$$

in cui $SE(\widehat{\beta_1})$ è la radice quadrata di uno stimatore della varianza della distribuzione campionaria di $\widehat{\beta_1}$. Nel nostro caso $\beta_{1,0} = 0$, quindi calcoliamo $t = \frac{\beta_1}{SE(\widehat{\beta_1})}$. Una volta determinata la statistica t si può rifiutare l'ipotesi H_0: $\beta_1 = 0$ secondo i seguenti criteri:

- se $|t| > 2{,}58$, si rifiuta H_0 al livello di significatività dell'1%;
- se $|t| > 1{,}96$, si rifiuta H_0 al livello di significatività del 5%;
- se $|t| > 1{,}28$, si rifiuta H_0 al livello di significatività del 10%.

Un altro metodo per accettare o rifiutare l'ipotesi nulla è quello di osservare il $p - value$, che indica la probabilità di rifiutare l'ipotesi quando in realtà è vera, ovvero la probabilità di rifiutare erroneamente H_0, e si valutano i seguenti casi:

- $p < 1\%$, si rifiuta H_0 al livello di significatività dell'1%;
- $p < 5\%$, si rifiuta H_0 al livello di significatività del 5%;
- $p < 10\%$, si rifiuta H_0 al livello di significatività del 10%.

La terza valutazione di accettazione o rifiuto di H_0 avviene attraverso gli intervalli di confidenza. Un intervallo di confidenza al 95% consiste nel range dei valori di β_1 che non può essere scartato da un test di ipotesi con un livello di significatività del 5%. È un intervallo, basato sui dati, che include il valore effettivo del parametro β_1 nel 95% dei casi nei campioni ripetuti (o ha una probabilità del 95% di contenere il vero valore di β_1) e viene costruito così:

$$intervallo\ di\ confidenza\ al\ 95\%\ per\ \beta_1 = \{\widehat{\beta_1} \pm 1{,}96 \times SE(\widehat{\beta_1})\}$$

Come anticipato, all'interno di questo intervallo è presente il valore reale del parametro β_1 e allora, se non contiene il valore 0, si può rifiutare l'ipotesi nulla H_0: $\beta_1 = 0$ al livello di significatività del 5%.

Un aspetto da tenere in considerazioni quando si fanno queste analisi è quello relativo alla eteroschedasticità e omoschedasticità dell'errore residuo. Nello specifico, se $var(u|X = x)$ è costante, ovvero se la varianza della distribuzione di u condizionata a X non dipende da X, allora u è detto omoschedastico. In caso contrario, u è eteroschedastico e comporta il fatto che la varianza di u dipende da X, che non dovrebbe succedere. Per ovviare a questo problema si passa a errori standard robusti, al fine di avere omoschedasticità. I modelli di regressione utilizzati per effettuare le diverse analisi con l'obiettivo di rispondere ai quesiti della ricerca utilizzano errori standard robusti all'eteroschedasticità, inserendo l'opzione "*robust*" su Stata. Se le assunzioni dei minimi quadrati ordinari, con l'aggiunta dell'ipotesi di omoschedasticità, sono valide, allora lo stimatore OLS è il più efficiente avendo la varianza minima tra tutti gli stimatori lineari.

È essenziale notare che nella pratica ci sono sempre variabili non considerate che possono causare distorsioni nello stimatore OLS. Questo errore u si verifica a causa di fattori o variabili che influenzano Y, ma non sono inclusi nella nostra equazione di regressione. Nella presente analisi, l'uso di un singolo regressore non è appropriato poiché si cerca di ottenere stime il più accurate possibile. Pertanto, si prova a identificare tutte le variabili incluse in u che potrebbero influenzare lo stimatore OLS e vengono inserite in un modello di regressione multipla. Nel contesto della regressione multipla, l'applicazione delle ipotesi sul coefficiente β_1 segue lo stesso principio utilizzato in una regressione con un solo regressore. Possiamo verificare tali ipotesi mediante la statistica-t tradizionale e costruire intervalli di confidenza $\{\widehat{\beta_1} \pm 1{,}96 \times SE(\widehat{\beta_1})\}$ e lo stesso vale per gli altri regressori $\beta_1, \dots, \beta_k$. Per cercare di inserire tutti i fattori omessi, vengono inserite le cosiddette "variabili di controllo" che sono correlate con Y e controllano per fattori causali omessi nella regressione ma che di per sé non hanno una effetto causale su Y.

3.3.2 Regressione logistica

Nel caso di variabile dipendente Y binaria si può utilizzare il modello lineare di probabilità in cui il valore predetto di Y è interpretato come la probabilità predetta che $Y = 1$ e β_1 è la variazione di tale probabilità generata da una variazione in Y. Quando Y è binaria, il modello lineare di regressione è chiamato modello lineare di probabilità e, nel caso di singolo regressore, è il seguente:

$$\Pr(Y = 1|X) = \beta_0 + \beta_1 X_i$$

Questo modello presenta alcune limitazioni, tra cui il fatto che la probabilità prevista di un determinato cambiamento in X rimane costante per tutti i valori di X, il che non è realisticamente plausibile. Inoltre, le probabilità previste possono cadere al di sotto di 0 o salire oltre 1, il che non è accettabile. Al contrario, ci si aspetta che il modello soddisfi queste condizioni.

- $\Pr(Y = 1|X)$ crescente in X per $\beta_1 > 0$
- $0 \leq \Pr(Y = 1|X) \leq 1$ per tutte le X

Per risolvere tale questione si possono usare modelli non lineari probabilità, tra cui la regressione *logit* che modella la probabilità che $Y = 1$ data X, utilizzando la funzione di ripartizione logistica standard F:

$$F(\beta_0 + \beta_1 X) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 X)}}$$

$$\Pr(Y = 1|X) = F(\beta_0 + \beta_1 X)$$

Il processo di stima si basa sul metodo della massima verosimiglianza (ML), dove la funzione di verosimiglianza rappresenta la probabilità congiunta dei dati. L'estimatore di massima verosimiglianza (MLE) è il valore di (β_0, β_1) che massimizza questa funzione, descrivendo così in modo ottimale l'intera distribuzione dei dati. In pratica, le stime ML rappresentano i valori dei parametri che, con maggiore probabilità, hanno generato quei dati specifici. La misura di bontà dell'adattamento utilizzata in questo contesto è la $Pseudo - R^2$, che riflette il miglioramento nel logaritmo della verosimiglianza rispetto a quando non ci sono variabili X nel modello.

4. Risultati dell'analisi econometrica

In questo capitolo andremo a studiare quali sono i fattori determinanti degli investimenti in cybersecurity nelle imprese del settore privato italiano sulla base dei dataset descritti precedentemente, cercando di analizzare la robustezza dei risultati nelle due indagini relative rispettivamente all'anno 2016 e 2022. In secondo luogo, in riferimento alle informazioni disponibili nell'anno 2016, si cercherà di valutare i drivers che influiscono sulla probabilità delle imprese a subire o meno un attacco informatico, e di studiare i fattori che favoriscono l'adozione di misure di difesa informatica specifiche. In terzo luogo, in riferimento all'anno 2022, si indagano i determinanti che inducono un'impresa ad avere più o meno consapevolezza di poter subire un attacco cibernetico. Di seguito, verranno riportate le specificazioni delle variabili utilizzate per effettuare le analisi, dei diversi modelli e dei relativi risultati per i due anni di riferimento.

4.1 Modelli empirici relativi all'indagine del 2016

4.1.1 Modello sugli investimenti in cybersecurity

Il primo modello che andiamo a studiare è quello relativo ai determinanti che influenzano gli investimenti in cybersecurity nelle imprese facendo riferimento all'indagine del 2016. In Tabella 5 sono riportate le variabili utilizzate nel modello.

Variabile dipendente	**Descrizione**
Investimenti	Intervallo della spesa sostenuta nel 2016 per tutelarsi dal rischio di attacchi informatici (1=Nessuna spesa; 2=Meno di 10.000; 3=Da 10.000 a 49.999; 4=Da 50.000 a 199.999; 5=200.000 e oltre)
Variabili indipendenti	**Descrizione**
Grande	Dummy che indica se l'impresa possiede 1000 e oltre dipendenti (0=No; 1=Sì)
Sud	Dummy che indica se l'impresa ha sede al Sud o nelle Isole (0=No; 1=Sì)
Manifatturiero	Dummy che indica se l'impresa appartiene al settore manifatturiero (0=No; 1=Sì)
Servizi	Dummy che indica se l'impresa appartiene al settore dei servizi non finanziari (0=No; 1=Sì)
EsportazioniBasse	Dummy che indica se l'impresa esporta meno di 1/3 del fatturato generato (0=No; 1=Sì)
AttaccoCyber	Dummy che indica se l'impresa ha subito attacchi informatici nel 2016 (0=No; 1=Sì)
DannoBasso	Dummy che indica se il danno arrecato dagli attacchi informatici subiti nel 2016 è inferiore a 10.000 euro (0=No; 1=Sì)

Attacco_MisureRafforzate	Dummy che indica se l'impresa ha rafforzato le misure di sicurezza dopo aver subito attacchi (0=No; 1=Sì)

Tabella 5. Descrizione delle variabili utilizzate nel modello sugli investimenti in cybersecurity del 2016

I risultati dell'analisi sono riportati in Figura 82 ma procediamo a commentarli in ordine. In prima battuta è stato considerato il seguente modello di regressione lineare (1):

$$Investimenti = \beta_0 + \beta_1 Grande + \beta_2 Sud + \beta_3 Manifatturiero + \beta_4 Servizi + \beta_5 EsportazioniBasse + \beta_6 AttaccoCyber + u_i$$

Si osserva come il fatto di essere una grande impresa (con 1000 dipendenti e oltre) sia statisticamente significativo per cui si conferma l'ipotesi fatta durante l'analisi descrittiva per cui le grandi imprese sono maggiormente spinte ad investire in cybersecurity. È verificata anche l'ipotesi per cui le organizzazioni situate nel Sud (e nelle Isole) investano meno in sicurezza informatica. Infatti, la variabile Sud è statisticamente significativa in modo negativo rispetto alla spesa in cybersicurezza. Anche il settore è una variabile significativa rispetto alla variabile dipendente. I risultati mostrano come le imprese del settore manifatturiero investano significativamente di meno rispetto a quelle dei servizi. Bisogna anche sottolineare che le imprese che esportano meno sono spinte ad investire meno nelle misure di protezione informatica, probabilmente perché sono meno esposte ad attacchi proveniente fuori dal confine. Evidenza degna di essere segnalata è quella relativa alla variabile *AttaccoCyber* che risulta essere statisticamente significativa all'1%, suggerendo che l'aver subito un attacco nel corso dell'anno sia positivamente associato alla scelta di investire in cybersecurity.

Successivamente si è proceduto andando a considerare l'effetto della variabile *Attacco_MisureRafforzate* nel modello (2):

$$Investimenti = \beta_0 + \beta_1 Grande + \beta_2 Sud + \beta_3 Manifatturiero + \beta_4 Servizi + \beta_5 EsportazioniBasse + \beta_6 Attacco\_MisureRafforzate + u_i$$

In questo caso, si mantiene la significatività delle variabili relative alla dimensione, all'area geografica e alla quota di esportazione, mentre si perde quella riferita al settore. È importante osservare come la scelta di rafforzare le misure di difesa in seguito ad un attacco cibernetico non sia statisticamente significativa.

Il passo dopo è stato valutare l'impatto dell'ammontare del danno patrimoniale subito in seguito ad un attacco cyber. Questo è stato possibile considerando la variabile *DannoBasso* nel modello (3):

$$Investimenti = \beta_0 + \beta_1 Grande + \beta_2 Sud + \beta_3 Manifatturiero + \beta_4 Servizi + \beta_5 EsportazioniBasse + \beta_6 DannoBasso + u_i$$

Il risultato ha suggerito come le imprese che hanno ricevuto un danno economico relativamente contenuto (inferiore a 10.000 euro) investono di meno rispetto a quelle che hanno subito un elevato danno, cioè l'entità del danno è proporzionale all'investimento in protezione.

Infine, sono state inserite sia la variabile di costo del danno che quella di attacco subito con relativa scelta di rafforzare le misure nel modello (4):

$$Investimenti = \beta_0 + \beta_1 Grande + \beta_2 Sud + \beta_3 Manifatturiero + \beta_4 Servizi + \beta_5 EsportazioniBasse + \beta_6 DannoBasso + \beta_7 Attacco\_MisureRafforzate + u_i$$

Le analisi evidenziano come le imprese di grandi dimensioni, con oltre 1000 dipendenti, siano notevolmente propense ad investire nella sicurezza informatica. Inoltre, si è riverificata l'ipotesi che le aziende situate nel Sud e nelle Isole investano meno nella protezione cibernetica, dato che la variabile geografica *Sud* è risultata statisticamente significativa all'1%, mostrando un effetto negativo sulla spesa in sicurezza informatica. Il settore industriale si è rivelato un fattore rilevante in relazione alla spesa in sicurezza informatica per le imprese che operano nel manifatturiero: i risultati indicano che le imprese manifatturiere tendono a investire in modo meno significativo rispetto a quelle dei servizi. Inoltre, le aziende con minori esportazioni sembrano essere meno propense a investire in misure di protezione informatica, per i motivi suggeriti precedentemente.

Risulta interessante notare che le imprese che hanno subito danni economici relativamente limitati (inferiori a 10.000 euro) non si sentano incentivate ad allocare risorse finanziarie per migliorare la loro cybersecurity e, infatti, la variabile *DannoBasso* è statisticamente significativa al 5% con un impatto negativo sulla variabile dipendente. Tuttavia, è cruciale sottolineare che in questo modello la decisione di rafforzare le misure di difesa dopo un attacco informatico è significativa da un punto di vista statistico. La variabile dummy che indica il rafforzamento o meno delle misure dopo un attacco hacker può essere intesa come una misura della consapevolezza della minaccia cyber e della possibilità di poter subire nuovamente in futuro un'altra violazione. Risulta allora che le imprese maggiormente consapevoli del rischio cyber sono propense ad investire maggiormente in cybersecurity.

VARIABLES	(1) Investimenti	(2) Investimenti	(3) Investimenti	(4) Investimenti
Grande	1,12***	1,13***	1,03***	1,02***
	(0,09)	(0,13)	(0,14)	(0,14)
Sud	-0,36***	-0,28***	-0,28***	-0,28***
	(0,05)	(0,09)	(0,10)	(0,09)
Manifatturiero	-0,38***	-0,21	-0,36*	-0,37*
	(0,14)	(0,24)	(0,28)	(0,28)
Servizi	-0,22*	0,01	-0,20	-0,21
	(0,14)	(0,25)	(0,28)	(0,29)
EsportazioniBasse	-0,22***	-0,36***	-0,33***	-0,32***
	(0,05)	(0,09)	(0,10)	(0,10)
AttaccoCyber	0,23***			
	(0,05)			
DannoBasso			-0,17*	-0,20**
			(0,09)	(0,09)
Attacco_MisureRafforzate		0,14		0,19*
		(0,14)		(0,15)
Costante	2,93***	2,92***	3,29***	3,14***
	0,15	(0,29)	(0,30)	0,35
R-squared	0,2182	0,2408	0,2247	0,2337

Errori standard robusti in parentesi
***p<0.01, **p<0.05, *p<0.1

Figura 82. Determinanti degli investimenti in cybersecurity, regressione lineare (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016])

4.1.2 Modello sulla probabilità di subire un attacco cyber

Il modello che studia gli effetti sulla probabilità di subire un attacco cyber in una impresa è basato sulla regressione logistica (logit), in cui la variabile dipendente *AttaccoCyber* è una dummy che indica se è stato subito un attacco nel corso del 2016. L'obiettivo è indagare i fattori che fanno aumentare o diminuire la probabilità di subire un cyber-attacco. Le variabili utilizzate sono riportante nella Tabella 6 seguente:

Variabile dipendente	**Descrizione**
AttaccoCyber	Dummy che indica se l'impresa ha subito attacchi informatici nel 2016 (0=No; 1=Sì)
Variabili indipendenti	**Descrizione**
Piccola	Dummy che indica se l'impresa possiede 20-49 dipendenti (0=No; 1=Sì)
Sud	Dummy che indica se l'impresa ha sede al Sud o nelle Isole (0=No; 1=Sì)
Manifatturiero	Dummy che indica se l'impresa appartiene al settore manifatturiero (0=No; 1=Sì)

Servizi	Dummy che indica se l'impresa appartiene al settore dei servizi non finanziari (0=No; 1=Sì)
EsportazioneMedia	Dummy che indica se l'impresa esporta tra 1/3 e 2/3 del fatturato generato (0=No; 1=Sì)
EsportazioneAlta	Dummy che indica se l'impresa esporta oltre 2/3 del fatturato generato (0=No; 1=Sì)
SoftwareSicurezza	Dummy che indica se l'impresa adotta software e/o hardware di sicurezza (0=No; 1=Sì)
FormazioneICT	Dummy che indica se l'impresa adotta formazione ICT del personale (0=No; 1=Sì)
CifraturaDati	Dummy che indica se l'impresa adotta cifratura completa o parziale dei dati (0=No; 1=Sì)
GestioneSistemi	Dummy che indica se l'impresa adotta analisi e gestione delle vulnerabilità dei sistemi aziendali (0=No; 1=Sì)
Investimenti	Investimenti in sicurezza informatica nel corso del 2016 (migliaia di euro)

Tabella 6. Descrizione delle variabili utilizzate nel modello sulla probabilità di subire un attacco cyber del 2016

L'analisi dei risultati procede inserendo progressivamente nuove variabili nel modello. Nel primo modello (1) sono considerate le variabili che caratterizzano l'impresa:

$$Prob\,(AttaccoCyber = 1) = \beta_0 + \beta_1 Piccola + \beta_2 Sud + \beta_3 Manifatturiero + \beta_4 Servizi + \beta_5 EsportazioneMedia + \beta_6 EsportazioneAlta + u_i$$

Le imprese di piccole dimensioni (tra 20 e 49 dipendenti) hanno una minore probabilità di subire un attacco informatico probabilmente perché sono percepite dagli attaccanti di valore inferiore rispetto ai guadagni che potrebbero trarre nell'attaccare una grande impresa e, infatti, la probabilità si riduce del 36%. Lo stesso si verifica per le organizzazioni che hanno sede nel Sud o Isole che potrebbero apparire meno attraenti agli hacker, a tal punto da ridurre la probabilità del 18%. Il settore non è statisticamente significativo sulla probabilità di subire un attacco, mentre la quota di esportazione è una variabile statisticamente significativa: in particolare, le imprese che esportano più di due terzi del fatturato hanno maggiore possibilità di essere bersagli di un attacco, la cui probabilità aumenta del 29%. La motivazione della maggiore esposizione oltre confine è sostenuta anche in questa analisi.

Nel secondo modello (2) vengono aggiunte le variabili che indicano l'adozione o meno di misure di difesa specifiche per vedere quali tra queste permette di ridurre la probabilità di subire un attacco:

$$Prob\ (AttaccoCyber = 1)$$
$$= \beta_0 + \beta_1 Piccola + \beta_2 Sud + \beta_3 Manifatturiero + \beta_4 Servizi$$
$$+ \beta_5 EsportazioneMedia + \beta_6 EsportazioneAlta$$
$$+ \beta_7 SoftwareSicurezza + \beta_8 FormazioneICT + \beta_9 CifraturaDati$$
$$+ \beta_{10} GestioneSistemi + u_i$$

Si può notare come, in questo caso, l'area geografica del Sud perda significatività statistica, mentre la dimensione piccola e l'esportazione alta rimangono significative. Per quanto riguarda le misure di difesa adottate, l'unica che è statisticamente significativa è quella che comprende l'analisi e gestione delle vulnerabilità dei sistemi aziendali (al livello di significatività dell'1%). L'indagine specifica come questa misura difensiva debba essere intesa come la capacità di elaborare un'analisi approfondita dei sistemi aziendali insieme alle relative politiche di sicurezza, al fine di identificare eventuali vulnerabilità che potrebbero renderli suscettibili a attacchi. Queste vulnerabilità possono derivare da errori di configurazione hardware, credenziali di accesso non aggiornate o troppo permissive, l'utilizzo di software notoriamente vulnerabili, e così via. Una volta individuate, queste vulnerabilità vengono corrette, e in alcuni casi, vengono effettuate simulazioni di attacco per valutare la resistenza del sistema in condizioni simili a un attacco reale. Visto l'impatto che l'adozione di tale misura è significativo (la probabilità aumenta del 48%) si potrebbe anche pensare che le imprese che dispongono di tali capacità siano maggiormente in grado di rilevare un attacco. Quindi, piuttosto che aumentare la probabilità di subire un attacco si può intendere che aumenta la capacità di riuscire a rilevare un attacco cyber.

Nel terzo modello (3) viene aggiunta la variabile sugli investimenti in cybersecurity effettuati per osservare se investire impatta la probabilità di subire una violazione o meno:

$$Prob\ (AttaccoCyber = 1)$$
$$= \beta_0 + \beta_1 Piccola + \beta_2 Sud + \beta_3 Manifatturiero + \beta_4 Servizi$$
$$+ \beta_5 EsportazioneMedia + \beta_6 EsportazioneAlta$$
$$+ \beta_7 SoftwareSicurezza + \beta_8 FormazioneICT + \beta_9 CifraturaDati$$
$$+ \beta_{10} GestioneSistemi + \beta_{11} Investimenti + u_i$$

La variabile sugli investimenti in cybersecurity (in migliaia di euro) è significativa al 10% ma ci si aspetterebbe che l'impatto fosse negativo, ovvero che all'aumentare dell'investimento in cybersicurezza diminuisca la probabilità di subire un attacco perché si hanno misure migliori per la difesa informatica. In questo caso, invece, l'impatto è positivo. La giustificazione di tale incoerenza può essere quella per cui le imprese adottano

maggiormente un approccio reattivo piuttosto che proattivo, ossia di investire solo in seguito ad aver subito un attacco e non prima per prevenire. Come è stato visto nel modello (1) del capitolo precedente, aver subito un attacco è un determinante della scelta di investire in cybersecurity. Inoltre, si deve fare notare che potrebbe esserci anche un'altra motivazione: le imprese più "appetibili" investono di più per difendersi, e al tempo stesso attraggono più facilmente degli attacchi (c'è un problema di endogeneità che non si sta affrontando con gli OLS). I risultati numerici delle analisi appena commentate si trovano in Figura 83.

	(1)	(2)	(3)
VARIABLES	AttaccoCyber	AttaccoCyber	AttaccoCyber
Piccola	-0,36***	-0,23**	-0,26*
	(0,08)	(0,09)	(0,14)
Sud	-0,18**	-0,10	-0,23*
	(0,08)	(0,09)	(0,15)
Manifatturiero	-0,14	-0,09	0,21
	(0,19)	(0,20)	(0,36)
Servizi	-0,06	-0,06	0,16
	(0,19)	(0,20)	(0,37)
EsportazioneMedia	0,11	0,07	0,20
	(1,03)	(0,11)	(0,18)
EsportazioneAlta	0,29***	0,27**	0,32*
	(0,11)	(0,11)	(0,18)
SoftwareSicurezza		0,29	-0,27
		(0,46)	(0,68)
FormazioneICT		0,14	0,21
		(0,10)	(0,16)
CifraturaDati		0,11	0,07
		(0,09)	(0,14)
GestioneSistemi		0,48***	0,55***
		(0,10)	(0,16)
Investimenti			0,0000995*
			(0,0000643)
Costante	-0,74***	-1,56***	-1,49**
	(0,18)	(0,48)	(0,72)
Pseudo R-squared	0,0103	0,024	0,0359

Errori standard robusti in parentesi
***p<0.01, **p<0.05, *p<0.1

Figura 83. Probabilità di subire un attacco, regressione logistica (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016])

4.1.3 Modello sull'adozione di misure difensive

Il seguente modello di regressione logistica ha l'obiettivo di valutare quali variabili possono spingere le imprese ad adottare o meno misure di sicurezza specifiche. come si può vedere in Tabella 7.

Variabile dipendente	**Descrizione**
SoftwareSicurezza	Dummy che indica se l'impresa adotta software e/o hardware di sicurezza (0=No; 1=Sì)
FormazioneICT	Dummy che indica se l'impresa adotta formazione ICT del personale (0=No; 1=Sì)
CifraturaDati	Dummy che indica se l'impresa adotta cifratura completa o parziale dei dati (0=No; 1=Sì)
GestioneSistemi	Dummy che indica se l'impresa adotta analisi e gestione delle vulnerabilità dei sistemi aziendali (0=No; 1=Sì)
Variabili indipendenti	**Descrizione**
Piccola	Dummy che indica se l'impresa possiede meno di 20-49 dipendenti (0=No; 1=Sì)
Sud	Dummy che indica se l'impresa ha sede al Sud o nelle Isole (0=No; 1=Sì)
Manifatturiero	Dummy che indica se l'impresa appartiene al settore manifatturiero (0=No; 1=Sì)
Servizi	Dummy che indica se l'impresa appartiene al settore dei servizi non finanziari (0=No; 1=Sì)
EsportazioneMedia	Dummy che indica se l'impresa esporta tra 1/3 e 2/3 del fatturato generato (0=No; 1=Sì)
EsportazioneAlta	Dummy che indica se l'impresa esporta oltre 2/3 del fatturato generato (0=No; 1=Sì)
Attacco_MisureRafforzate	Dummy che indica se l'impresa ha rafforzato le misure di sicurezza dopo aver subito attacchi (0=No; 1=Sì)

Tabella 7. Descrizione delle variabili utilizzate nel modello sulla probabilità di adottare misure difensive specifiche del 2016

Il modello di regressione logistica è il seguente:

$$Prob\,(Y = 1) = \beta_0 + \beta_1 Piccola + \beta_2 Sud + \beta_3 Manifatturiero + \beta_4 Servizi + \beta_5 EsportazioneMedia + \beta_6 EsportazioneAlta + \beta_7 Attacco\_MisureRafforzate + u_i$$

in cui Y può essere una delle variabili che indicano l'adozione o meno di una delle misure di sicurezza, ovvero $SoftwareSicurezza$, $FormazioneICT$, $CifraturaDati$ o $GestioneSistemi$.

Dai risultati in Figura 84, si può constatare che le piccole imprese sono meno propense ad adottare misure di difesa specifiche osservando che la variabile *Piccola* è in tutti i casi statisticamente significativa negativa. Anche la variabile *Sud* è statisticamente significativa con un effetto negativo sull'adozione delle misure difensive specifiche, ad eccezione dei software e/o hardware di sicurezza. Dall'analisi descrittiva si era visto come il 99% delle imprese rispondenti avessero adottato tale misura di difesa cyber. Un risultato coerente con l'ipotesi per cui le imprese che operano nel settore dei servizi (non finanziari) abbiano la necessità di disporre di misure di protezione informatica migliori è che la variabile *Servizi* è statisticamente significativa con effetto positivo. L'adozione della cifratura dei dati è favorita nelle organizzazioni esportatrici: le variabili sulla quota di esportazione sono entrambe statisticamente significative con un effetto positivo sulla scelta di azione. La spiegazione segue quella sulla scelta di investire per le organizzazioni che esportano oltre confine: queste imprese vogliono garantire un livello di sicurezza elevato e una protezione adeguata delle informazioni sensibili con l'utilizzo di tecnologie di cifratura che permette di proteggere le comunicazioni e i dati sensibili durante la loro trasmissione attraverso la rete, impedendo agli hacker di intercettare o manipolare le informazioni. Ciò è particolarmente cruciale per le imprese che operano a livello internazionale, dove i dati possono attraversare confini nazionali ed essere soggetti a diverse normative sulla privacy. Adottare la cifratura dei dati non solo protegge la reputazione dell'azienda, ma contribuisce anche a mantenere la fiducia dei clienti e dei partner commerciali. Di fronte ad un attacco cyber, la scelta di rafforzare la difese è significativa sull'adozione delle misure. La decisione di migliorare le difese dopo un attacco è sinonimo di consapevolezza dell'impresa della possibile minaccia cyber che potrebbe giungere nel futuro e, allora, le imprese che sono consapevoli che nessuna può evitare tali violazioni adottano misure di difesa con maggiore probabilità.

VARIABLES	(1) SoftwareSicurezza	(2) FormazioneICT	(3) CifraturaDati	(4) GestioneSistemi
Piccola	-1,71*	-0,83***	-0,89***	-0,65***
	(1,19)	(0,17)	(0,17)	(0,17)
Sud	-0,72	-0,26*	-0,43***	-0,74***
	(0,93)	(0,17)	(0,16)	(0,17)
Manifatturiero	-12,97***	0,33	0,40	0,31
	(0,68)	(0,33)	(0,37)	(0,35)
Servizi	-12,71***	0,51*	0,99***	0,78**
	(1,22)	(0,34)	(0,37)	(0,35)
EsportazioneMedia	-1,65*	-0,04	0,35*	-0,06
	(0,92)	(0,23)	(0,19)	(0,21)
EsportazioneAlta	-1,72*	0,05	0,30*	0,23
	(1,19)	(0,22)	(0,19)	(0,21)
Attacco_MisureRafforzate	1,90**	0,84***	0,22	0,73***
	(0,85)	(0,21)	(0,22)	(0,21)
Costante	18,62***	0,49*	-0,79**	0,33
	(0,97)	(0,35)	(0,38)	(0,37)
Pseudo R-squared	0,1718	0,0542	0,056	0,0678

Errori standard robusti in parentesi
***p<0.01, **p<0.05, *p<0.1

Figura 84. Probabilità di adottare misure difensive, regressione logistica (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2016])

4.2 Modelli empirici relativi all'indagine del 2022

4.2.1 Modello sugli investimenti in cybersecurity

Il modello che segue cerca di studiare i fattori che impattano la scelta di un'impresa di investire in cybersecurity. Le variabili indipendenti su dimensione, area, settore ed esportazioni sono presenti anche nella relativa indagine del 2022 ma le variabili riferite al tema della cybersicurezza sono cambiate in parte. Infatti, nel questionario sottoposto alle imprese non sono presenti esattamente le stesse domande ma è possibile comunque fare osservazioni dai risultati e valutare se ci sono stati cambiamenti nel corso degli anni. Nessun'altra indagine tra il 2016 e il 2022 condotta da Banca d'Italia ha inserito una sezione dedicata al tema della cybersecurity. Da quella in esame sono state individuate come utili allo studio le variabili in Tabella 8.

Variabile dipendente	Descrizione
Investimenti	Intervallo della spesa sostenuta nel biennio 2021-2022 per tutelarsi dal rischio di attacchi cibernetici (1=Nessuna spesa; 2=Fino a 5.000€; 3=Da 5.001€ a 10.000€; 4=Da 10.001€ a 50.000€; 5=Da 50.001€ a 200.000€; 6=Oltre 200.000)

Variabili indipendenti	Descrizione
Grande	Dummy che indica se l'impresa possiede 1000 e oltre dipendenti (0=No; 1=Sì)
Sud	Dummy che indica se l'impresa ha sede al Sud o nelle Isole (0=No; 1=Sì)
Manifatturiero	Dummy che indica se l'impresa appartiene al settore manifatturiero (0=No; 1=Sì)
Servizi	Dummy che indica se l'impresa appartiene al settore dei servizi non finanziari (0=No; 1=Sì)
EsportazioniBasse	Dummy che indica se l'impresa esporta meno di 1/3 del fatturato generato (0=No; 1=Sì)
ConsapevolezzaAttacco	Dummy che indica se l'impresa ritiene molto probabile subire attacchi cibernetici (0=No; 1=Sì)
NoVariazioneSpesa	Dummy che indica se l'impresa negli ultimi 5 anni non ha aumentato la spesa in sicurezza informatica (0=No; 1=Sì)
NoAttaccoCyber	Dummy che indica se l'impresa negli ultimi 5 anni non ha subito attacchi cibernetici (0=No; 1=Sì)
Attacco_DannoCyber	Dummy che indica se l'impresa negli ultimi 5 anni ha subito danni patrimoniali in seguito ad attacchi cibernetici (0=No; 1=Sì)
NoFunzione	Dummy che indica se l'impresa non possiede una funzione aziendale dedicata alla gestione della cybersicurezza (0=No; 1=Sì)
Outsourcing	Dummy che indica se l'impresa possiede una funzione aziendale dedicata alla gestione della cybersicurezza in outsourcing (0=No; 1=Sì)

Tabella 8. Descrizione delle variabili utilizzate nel modello sulla probabilità di subire un attacco cyber del 2021-2022

Le regressioni (1) e (2) vogliono indagare l'impatto del non aver subito un attacco sulla decisione di investire o meno in sicurezza informatica:

$$Investimenti = \beta_0 + \beta_1 Grande + \beta_2 Sud + \beta_3 Manifatturiero + \beta_4 Servizi + \beta_5 EsportazioniBasse + \beta_6 ConsapevolezzaAttacco + \beta_7 NoVariazioneSpesa + \beta_8 NoAttaccoCyber + \beta_9 NoFunzione + u_i$$

$$Investimenti = \beta_0 + \beta_1 Grande + \beta_2 Sud + \beta_3 Manifatturiero + \beta_4 Servizi + \beta_5 EsportazioniBasse + \beta_6 ConsapevolezzaAttacco + \beta_7 NoVariazioneSpesa + \beta_8 NoAttaccoCyber + \beta_9 Outsourcing + u_i$$

Risulta (Figura 85) che la dimensione, l'area geografica e la quota di esportazioni siano statisticamente significative. In particolare, le imprese di grandi dimensioni (con oltre 1.000 addetti) sono più inclini ad investire e la variabile *Grande* è significativa all'1% con effetto positivo. Poi, si osserva che le imprese del meridione investano minori somme per la cybersecurity e questo è confermato dalla variabile *Sud* che è significativa all'1% con un effetto negativo sulla variabile dipendente degli investimenti. Le imprese che esportano poco

(meno di 1/3 del fatturato generato), anche in questo caso, decidono di investire meno rispetto alle grandi esportatrici. Infatti, la variabile *EsportazioniBasse* è significativa all'1% con impatto negativo. Il settore non gioca un ruolo di impatto statisticamente significativo sugli investimenti cyber. Un'impresa che ha la consapevolezza che, con molta probabilità, possa subire un attacco informatico investe in cybersecurity per avere i mezzi per rilevare, affrontare e monitorare una violazione informatica in maniera efficiente. La variabile *ConsapevolezzaAttacco* è significativa all'1% e ha un effetto positivo sugli investimenti. Le imprese che decidono di effettuare investimenti cyber non dovrebbero farlo una tantum ma piuttosto creare un piano di investimenti che duri negli anni per cercare di migliorare costantemente la propria capacità difensiva visti i trend di crescita negli attacchi informatici in Italia e nei metodi in cui gli hacker attaccano le organizzazioni. I risultati evidenziano che le imprese che non hanno aumentato la spesa in cybersicurezza negli ultimi cinque anni, decidono di investire meno rispetto alle altre. Si osserva che la variabile *NoVariazioneSpesa* è statisticamente significativa e ha un impatto negativo. Allo stesso modo, le imprese che non hanno subito un attacco cibernetico nei precedenti cinque anni allocano minore budget per migliorare le difese informatiche (la variabile *NoAttaccoCyber* è significativa all'1% e ha effetto negativo). Probabilmente, questo può essere giustificato dal fatto che, non avendo subito una violazione negli anni prima, ritengano le proprie difese adeguate oppure la propria organizzazione non interessante agli scopi degli attaccanti. Le imprese possono disporre di una funzione aziendale (anche eventualmente in outsourcing) dedicata al governo e alla gestione della cybersicurezza e della continuità operativa e questo può influire gli investimenti in cybersecurity. Dai risultati si può osservare che le organizzazioni che non dispongono di tale funzione siano meno propense ad investire in cybersecurity. Possedere o meno una funzione aziendale dedicata alla cybersicurezza indica una attenzione dell'impresa verso la tematiche della sicurezza informatica e, quindi, è coerente che le imprese che non dispongono di tale funzione siano meno propense ad investire. Infine, avere questa funzione gestita completamente in outsourcing non influenza la scelta o meno di investire perché le imprese preferiscono destinare a terzi i compiti e le responsabilità piuttosto che gestirle internamente.

Nei risultati delle regressioni (3) e (4) si osserva come l'aver subito un danno patrimoniale in seguito ad un attacco cyber nei cinque anni precedenti non sia un determinante significativo nella scelta di investire o meno in cybersecurity. Le altre conclusioni sono in linea con quelle delle regressioni (1) e (2). L'unica eccezione è fatta dal settore

manifatturiero, per cui le imprese che operano in tale settore sono meno incentivate ad investire in cybersicurezza. La variabile *Manifatturiero* è significativa al 10% e ha un impatto negativo sugli investimenti cyber. Di seguito le regressioni (3) e (4) rispettivamente:

$$Investimenti = \beta_0 + \beta_1 Grande + \beta_2 Sud + \beta_3 Manifatturiero + \beta_4 Servizi + \beta_5 EsportazioniBasse + \beta_6 ConsapevolezzaAttacco + \beta_7 NoVariazioneSpesa + \beta_8 Attacco\_DannoCyber + \beta_9 NoFunzione + u_i$$

$$Investimenti = \beta_0 + \beta_1 Grande + \beta_2 Sud + \beta_3 Manifatturiero + \beta_4 Servizi + \beta_5 EsportazioniBasse + \beta_6 ConsapevolezzaAttacco + \beta_7 NoVariazioneSpesa + \beta_8 Attacco\_DannoCyber + \beta_9 Outsourcing + u_i$$

VARIABLES	(1) Investimenti	(2) Investimenti	(3) Investimenti	(4) Investimenti
Grande	1,12***	1,14***	1,16***	1,18***
	(0,13)	(0,14)	(0,14)	(0,14)
Sud	-0,22***	-0,26***	-0,22***	-0,25***
	(0,05)	(0,05)	(0,05)	(0,05)
Manifatturiero	-0,15	-0,16	-0,18*	-0,19*
	(0,13)	(0,14)	(0,14)	(0,14)
Servizi	-0,01	-0,01	-0,03	-0,03
	(0,13)	0,14	(0,14)	(0,14)
EsportazioniBasse	-0,34***	-0,36***	-0,36***	-0,39***
	(0,06)	(0,06)	(0,06)	(0,06)
ConsapevolezzaAttacco	0,66***	0,70***	0,77***	0,83***
	(0,06)	(0,07)	(0,06)	(0,06)
NoVariazioneSpesa	-1,08***	-1,22***	-1,12***	-1,28***
	(0,06)	(0,05)	(-0,06)	(0,05)
NoAttaccoCyber	-0,32***	-0,37***		
	(0,06)	(0,06)		
Attacco_DannoCyber			-0,08	-0,05
			(0,10)	(0,10)
NoFunzione	-0,50***		-0,53***	
	(0,05)		(0,05)	
Outsourcing		0,02		0,00
		(0,07)		0,07
Costante	3,81***	3,77***	3,62***	3,55***
	(0,15)	(0,16)	(0,15)	(0,16)
R-squared	0,5292	0,5067	0,5210	0,4954

Errori standard robusti in parentesi
***p<0.01, **p<0.05, *p<0.1

Figura 85. Determinanti degli investimenti in cybersecurity, regressione lineare (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

4.2.2 Modello sulla consapevolezza di subire un attacco cyber

Nel prossimo modello si vuole studiare quali sono i fattori che impattano la consapevolezza di un'impresa della possibile minaccia cyber. Questa misura è data da una scala da 1 a 3 che indica quanto l'impresa ritenga probabile possa subire un attacco cibernetico. In Tabella 9 sono riportate le variabili usate nel modello di regressione lineare:

Variabile dipendente	**Descrizione**
ConsapevolezzaAttacco	Misura di quanto l'impresa ritenga probabile possa subire attacchi cibernetici? (1=Per nulla probabile; 2=Poco probabile; 3=Molto probabile)
Variabili indipendenti	**Descrizione**

Grande	Dummy che indica se l'impresa possiede 1000 e oltre dipendenti (0=No; 1=Sì)
Sud	Dummy che indica se l'impresa ha sede al Sud o nelle Isole (0=No; 1=Sì)
Manifatturiero	Dummy che indica se l'impresa appartiene al settore manifatturiero (0=No; 1=Sì)
Servizi	Dummy che indica se l'impresa appartiene al settore dei servizi non finanziari (0=No; 1=Sì)
Esportazioni	Dummy che indica se l'impresa esporta oltre 2/3 del fatturato generato (0=No; 1=Sì)
Investimenti	Intervallo della spesa sostenuta nel biennio 2021-2022 per tutelarsi dal rischio di attacchi cibernetici (1=Nessuna spesa; 2=Fino a 5.000€; 3=Da 5.001€ a 10.000€; 4=Da 10.001€ a 50.000€; 5=Da 50.001€ a 200.000€; 6=Oltre 200.000)
NoVariazioneSpesa	Dummy che indica se l'impresa negli ultimi 5 anni non ha aumentato la spesa in sicurezza informatica (0=No; 1=Sì)
NoAttaccoCyber	Dummy che indica se l'impresa negli ultimi 5 anni non ha subito attacchi cibernetici (0=No; 1=Sì)
DannoCyber	Dummy che indica se l'impresa negli ultimi 5 anni ha subito danni patrimoniali in seguito ad attacchi cibernetici (0=No; 1=Sì)
NoFunzione	Dummy che indica se l'impresa non possiede una funzione aziendale dedicata alla gestione della cybersicurezza (0=No; 1=Sì)
Outsourcing	Dummy che indica se l'impresa possiede una funzione aziendale dedicata alla gestione della cybersicurezza in outsourcing (0=No; 1=Sì)

Tabella 9. Descrizione delle variabili utilizzate nel modello sulla consapevolezza di poter subire un attacco cyber

Anche per rispondere a questo quesito si procede andando a considerare prima l'impatto del non aver subito attacchi cyber in (1) e (2) e poi l'effetto dell'aver subito danni patrimoniali in seguito ad attacchi in (3) e (4). Di seguito sono riportati i modelli di regressione lineare:

$$ConsapevolezzaAttacco = \beta_0 + \beta_1 Grande + \beta_2 Sud + \beta_3 Manifatturiero + \beta_4 Servizi + \beta_5 Esportazioni + \beta_6 Investimenti + \beta_7 NoVariazioneSpesa + \beta_9 NoAttaccoCyber + \beta_{10} NoFunzione + u_i$$

$$ConsapevolezzaAttacco = \beta_0 + \beta_1 Grande + \beta_2 Sud + \beta_3 Manifatturiero + \beta_4 Servizi + \beta_5 Esportazioni + \beta_6 Investimenti + \beta_7 NoVariazioneSpesa + \beta_9 NoAttaccoCyber + \beta_{10} Outsourcing + u_i$$

$$ConsapevolezzaAttacco = \beta_0 + \beta_1 Grande + \beta_2 Sud + \beta_3 Manifatturiero + \beta_4 Servizi + \beta_5 Esportazioni + \beta_6 Investimenti + \beta_7 NoVariazioneSpesa + \beta_9 Attacco\_DannoCyber + \beta_{10} NoFunzione + u_i$$

$$ConsapevolezzaAttacco = \beta_0 + \beta_1 Grande + \beta_2 Sud + \beta_3 Manifatturiero + \beta_4 Servizi + \beta_5 Esportazioni + \beta_6 Investimenti + \beta_7 NoVariazioneSpesa + \beta_9 Attacco\_DannoCyber + \beta_{10} Outsourcing + u_i$$

I risultati delle regressioni lineare sono riportati in Figura 86 e si osserva come in nessun caso la dimensione e l'area geografica siano fattori che determinano la consapevolezza o meno di un'impresa nei confronti della minaccia cyber. Il settore dei servizi è statisticamente significativo al 10% e ha un impatto positivo. Questo vuole dire che le imprese dei servizi sono maggiormente consapevoli rispetto a quelle manifatturiere della possibilità di poter subire una attacco cibernetico. Le imprese esportatrici (oltre 2/3 del fatturato) non sembrano essere consapevoli che sono maggiormente esposte agli attacchi cyber rispetto ad altre che non esportano. L'investimento in sicurezza informatica è un'indicazione dell'interesse e dell'attenzione di un'organizzazione nei confronti della cybersecurity. Infatti, la variabile *Investimenti* è statisticamente significativa all'1% e suggerisce che le aziende che investono di più hanno una consapevolezza superiore. Al contrario, quelle che non hanno aumentato la spesa investita in cybersicurezza nei precedenti cinque anni sono meno consapevoli. Infatti, la variabile *NoVariazioneSpesa* è significativa all'1% e ha un effetto negativo sulla consapevolezza. Discorso analogo è fatto per le imprese che non hanno subito attacchi negli scorsi cinque anni. Il non subire alcun attacco cibernetico può far pensare alle imprese che la minaccia informatica non sia effettivamente esistente e che non riguardi quelle imprese. La variabile *NoAttaccoCyber* è significativa all'1% con impatto negativo sulla variabile dipendente. Andando ad osservare la presenza o meno della funzione aziendale dedicata alla gestione della cybersicurezza, i risultati evidenziano come l'assenza di tale funzione sia un indicatore di una minore consapevolezza cyber. Le imprese che non dispongono di una funzione dedicata alla cybersecurity non riconoscono probabilmente l'importanza e l'esistenza concreta delle possibili minacce cyber. Infatti, la variabile *NoFunzione* ha un impatto negativo ed è significativa all'1%. Dall'altro lato, ci sono le imprese che decidono di destinare la funzione in outsourcing e che dimostrano avere quindi consapevolezza e

interesse nell'avere un ente terzo che si occupi della gestione cyber. Questo è provato dalla significatività della variabile *Outsourcing* con impatto positivo.

Nelle regressioni (3) e (4) si ritrovano i risultati analoghi rispetto alle variabili in comune considerate. Inserendo la variabile *Attacco_DannoCyber* il settore manifatturiero perde significatività statistica. Relativamente alla variabile inserita, si può notare come l'aver subito un danno economico in seguito ad un attacco cibernetico nei cinque anni antecedenti all'indagine aumenti la consapevolezza dell'impresa. Questo può essere giustificato dall'ipotesi per cui un'impresa che subisce un danno patrimoniale vede la minaccia cyber concreta e tangibile e, soprattutto, avendo già subito un attacco, si può sentire un bersaglio scelto degli attaccanti. Statisticamente parlando, la variabile è significativa all'1% e ha un impatto positivo sulla consapevolezza cyber.

	(1)	(2)	(3)	(4)
VARIABLES	ConsapevolezzaAttacco	ConsapevolezzaAttacco	ConsapevolezzaAttacco	ConsapevolezzaAttacco
Grande	-0,05	-0,06	-0,04	-0,04
	(0,05)	(0,05)	(0,05)	(0,05)
Sud	0,02	0,01	0,02	0,02
	(0,03)	(0,03)	(0,03)	(0,03)
Manifatturiero	0,09*	0,09*	0,07	0,07
	(0,06)	(0,06)	(0,06)	(0,06)
Servizi	0,11*	0,11*	0,10*	0,10*
	(0,06)	(0,06)	(0,06)	(0,06)
Esportazioni	-0,005	-0,001	-0,0002	-0,002
	(0,04)	(0,04)	(0,04)	(0,04)
Investimenti	0,14***	0,15***	0,17***	0,18***
	(0,01)	(0,01)	(0,01)	(0,01)
NoVariazioneSpesa	-0,14***	-0,16***	-0,16***	-0,18***
	(0,03)	(0,03)	(0,03)	(0,03)
NoAttaccoCyber	-0,30***	-0,31***		
	(0,03)	(0,03)		
Attacco_DannoCyber			0,32***	0,33***
			(0,05)	(0,05)
NoFunzione	-0,10***		-0,12***	
	(0,03)		(0,03)	
Outsourcing		0,05*		0,03
		(0,03)		(0,03)
Costante	1,96***	1,96***	1,73***	1,66***
	-0,08	(0,08)	(0,07)	(0,07)
R-squared	0,3369	0,3331	0,3067	0,3004

Errori standard robusti in parentesi
***p<0.01, **p<0.05, *p<0.1

Figura 86. Determinanti della consapevolezza di poter subire un attacco cyber, regressione lineare (Fonte: Banca d'Italia, Indagine sulle imprese industriali e dei servizi, [2022])

5. Conclusioni

Nel contesto di digitalizzazione e globalizzazione in cui le imprese si trovano a dover operare oggi, la cybersecurity ricopre sicuramente un ruolo chiave per il corretto funzionamento e sopravvivenza di una organizzazione. Il trend globale e, soprattutto, italiano sul numero di attacchi informatici è in crescita così come le capacità e abilità di hackeraggio dei malintenzionati che cercano di trarre benefici dal violare un'impresa. Di fronte a tale andamento, anche gli investimenti in cybersecurity delle imprese, italiane e no, sono in aumento per fronteggiare le minacce incombenti. Focalizzando l'attenzione sull'Italia, nel 2022 si è verificato un aumento notevole degli attacchi informatici rispetto al 2021 (+168,6% secondo il Rapporto Clusit). Alla fine del 2022, gli investimenti in cybersicurezza registrati sono stati pari a 1,86 milioni di euro, segnando l'incremento percentuale migliore degli ultimi cinque anni (+18% rispetto al 2021 secondo l'Osservatorio «Cybersecurity e data protection» del Politecnico di Milano). Tuttavia, in valore assoluto e guardando gli altri Paesi del G7, questa cifra è ancora la metà rispetto a quanto investono Germania, Francia, Canada e Giappone, e solo un terzo di quanto investono Stati Uniti e Regno Unito.

Facendo riferimento alle informazioni ottenute dalla indagini condotte da Banca d'Italia nel 2016 e nel 2022, si osserva come circa il 70% dei rispondenti abbiano dichiarato di non aver subito attacchi sia nel 2016 che negli ultimi cinque anni. Questa percentuale elevata potrebbe indicare che le imprese del campione non siano bersagli interessanti per gli attaccanti oppure non abbiano le capacità per rilevare un attacco cyber. Questa seconda ipotesi potrebbe essere motivata dal fatto che gli investimenti effettuati dalle imprese siano stati in entrambi gli anni di indagine relativamente contenuti: nel 2016 il 56% dei rispondenti ha riportato di aver investito meno di 10.000 euro (o di non aver effettuato alcuna spesa), mentre nel biennio 2021-2022 questa percentuale sale al 68%. Proprio la percentuale di imprese che non hanno investito in cybersecurity è aumentata dall'8% al 19%, indicazione della minore comprensione dell'importanza di investire in misure di difesa cyber. Dall'indagine del 2016 emerge come le imprese prediligano un atteggiamento reattivo, piuttosto che proattivo, quando si tratta di spendere per la cybersecurity: l'87% delle organizzazioni che hanno subito un attacco cibernetico ha deciso di rafforzare le misure di sicurezza. L'indagine condotta nel 2022 ha cercato di raccogliere informazioni in merito alle scelte sulla cybersecurity avvenute tra le imprese nei cinque anni precedenti. La variazione della spesa in cybersicurezza nell'arco di tempo valutato è stata nulla per il 44% delle imprese, mentre del restante in cui la variazione è stata crescente, il 16% ha raddoppiato gli investimenti. Il

fatto di non stabilire un aumento del budget dedicato al miglioramento della cybersecurity può essere motivato dalla consapevolezza che hanno le imprese di poter subire un attacco cibernetico: infatti, il 61% delle aziende pensa che sia altamente improbabile essere vittima di un attacco cibernetico, mentre il 10% ritiene addirittura impossibile che ciò accada. Anche il fatto che il 24% delle imprese che hanno subito una violazione non abbiano registrato una perdita patrimoniale disincentiva la decisione di aumentare gli investimenti in cybersicurezza. L'osservazione che solo il 5% abbia indicato di aver subito, oltre all'attacco, anche un danno economico fa pensare che molte aziende non dispongano di sistemi in grado di quantificare il danno effettivo causato dall'attacco.

Per quanto riguarda i quesiti della seguente ricerca, sono stati analizzati modelli di regressione lineare per indagare i determinanti degli investimenti in cybersecurity e della consapevolezza di poter subire un attacco cibernetico e modelli di regressione logistica per investigare i fattori che influenzano la probabilità di subire un attacco cyber e di adottare misure difensive specifiche.

L'analisi di regressione lineare condotta ha fornito importanti insight riguardo ai determinanti che influenzano gli investimenti nel settore cyber. I risultati indicano chiaramente che le dimensioni dell'impresa svolgono un ruolo cruciale, con le grandi aziende che mostrano una propensione significativamente maggiore ad investire in sicurezza cibernetica. Allo stesso tempo, la posizione geografica ha un impatto significativo, con le imprese situate nel Sud che investono meno rispetto a quelle nelle altre regioni. Inoltre, l'analisi ha rivelato che le aziende manifatturiere tendono ad investire meno, così come quelle che non esportano i loro prodotti. La presenza di attacchi cyber passati è stata identificata come un fattore positivo per gli investimenti, con le aziende colpite che tendono ad investire di più rispetto a quelle che non hanno subito attacchi. Tuttavia, il costo del danno subito gioca un ruolo significativo, con le aziende che investono meno se il danno è basso. Le imprese che rafforzano le loro misure di difesa e dimostrano una maggiore consapevolezza della minaccia mostrano una tendenza positiva ad investire di più. L'assenza di una funzione aziendale specifica e della variazione nella spesa non sembra essere determinante nella decisione di investire in sicurezza cibernetica, ma piuttosto ad investire meno. In conclusione, questi risultati forniscono una panoramica dettagliata sui fattori che guidano gli investimenti cyber, offrendo preziose indicazioni per le strategie future delle imprese nel contesto sempre più complesso della cybersecurity.

L'analisi di regressione logistica condotta ha rivelato una serie di fattori che influenzano significativamente la probabilità di subire un attacco cyber da parte delle aziende. In primo luogo, le imprese di piccole dimensioni appaiono essere meno suscettibili agli attacchi rispetto alle loro controparti più grandi. Allo stesso modo, le aziende situate nel Sud mostrano una minore probabilità di subire un attacco rispetto a quelle in altre regioni. In modo interessante, le imprese esportatrici sono più a rischio, indicando che potrebbero essere soggette a minacce più elevate a causa della loro attività internazionale. Un aspetto sorprendente emerso dall'analisi è che le aziende che dispongono di misure di gestione dei sistemi e delle vulnerabilità aziendali sembrano essere più inclini a subire attacchi o, almeno, a rilevarli. Questo risultato solleva importanti questioni riguardo all'efficacia delle attuali strategie di gestione della sicurezza informatica e sottolinea l'importanza di ulteriori indagini per comprendere appieno questa dinamica. In conclusione, questi risultati forniscono un quadro prezioso per le aziende e gli esperti di cybersecurity, offrendo indicazioni cruciali per sviluppare politiche e strategie mirate a ridurre la probabilità di subire attacchi cyber.

La seconda analisi di regressione logistica condotta ha offerto una profonda comprensione dei fattori che influenzano la probabilità delle aziende nell'adottare misure di difesa cyber. In primo luogo, è emerso che le aziende di piccole dimensioni hanno una minore propensione ad adottare tali misure, suggerendo che potrebbero essere più vulnerabili a minacce cyber a causa di risorse limitate o di una scarsa consapevolezza dei rischi. Allo stesso modo, le imprese situate nel Sud mostrano una minore inclinazione a implementare misure difensive, indicando possibili disparità regionali nell'adozione delle best practices di sicurezza informatica. Un aspetto interessante è che le aziende del settore dei servizi sono più propense a adottare misure difensive, probabilmente a causa della crescente consapevolezza dei rischi nel contesto dei servizi online e digitali. Inoltre, è stato osservato che le imprese che rafforzano le misure difensive dopo aver subito un attacco hanno una maggiore probabilità di adottare ulteriori misure difensive, un risultato che appare quasi scontato ma che conferma l'importanza dell'esperienza diretta nelle decisioni di sicurezza aziendale. In conclusione, questi risultati sottolineano l'importanza di strategie mirate per promuovere l'adozione diffusa di misure di difesa cyber, specialmente tra le piccole imprese e quelle situate in regioni geografiche specifiche, al fine di migliorare la resilienza delle aziende di fronte alle crescenti minacce cyber.

Per ultima, l'analisi di regressione lineare condotta ha permesso di identificare chiaramente i fattori che influiscono sulla consapevolezza delle aziende riguardo alla possibilità di subire

un attacco cyber. Le imprese del settore dei servizi risultano essere più consapevoli, probabilmente a causa della crescente esposizione al mondo digitale e alla consapevolezza dei rischi ad essa associati. Inoltre, è emerso che le aziende che investono in sicurezza cibernetica dimostrano una maggiore consapevolezza, sottolineando l'importanza degli investimenti preventivi. La variazione nella spesa nel corso dei cinque anni precedenti è emersa come un indicatore significativo, con le imprese che non hanno variato la spesa risultano meno consapevoli. Allo stesso tempo, le aziende che non hanno subito attacchi cyber negli ultimi cinque anni appaiono meno consapevoli dei rischi, suggerendo una possibile mancanza di esperienza diretta. Interessante è il fatto che le imprese che hanno subito danni patrimoniali a seguito di attacchi cyber mostrano una maggiore consapevolezza, indicando che le conseguenze finanziarie possono svolgere un ruolo educativo significativo. Infine, la presenza di una funzione aziendale dedicata alla sicurezza cyber sembra essere un determinante importante, con le aziende che non la hanno risultano meno consapevoli. In conclusione, questi risultati sottolineano l'importanza di promuovere la consapevolezza dei rischi cyber tra le aziende e di incoraggiare gli investimenti in sicurezza informatica per affrontare le minacce sempre crescenti nel mondo.

Nell'attuale contesto è importante aumentare gli investimenti in cybersecurity delle imprese e si rivela quindi fondamentale implementare una combinazione di incentivi e politiche che promuovano la consapevolezza sulla sicurezza informatica, riducano i rischi e offrano vantaggi economici alle imprese che decidono di investire in tale campo. Sicuramente sarebbe importante esistessero incentivi fiscali attraverso crediti d'imposta o deduzioni fiscali per le imprese che investono in cybersecurity al fine di coprire una parte dei costi sostenuti. Anche le agevolazioni finanziarie basate su programmi di prestiti a tasso agevolato per le imprese che vogliono investire in misure di sicurezza informatica potrebbero essere una via efficacie. Una componente che andrebbe sostenuta è quella relativa alla ricerca e sviluppo per cercare di trovare soluzioni all'avanguardia e in grado di proteggere le imprese dalle minacce sempre più sofisticate. Vista l'esistenza di norme standard di sicurezza potrebbe essere utile creare incentivi per le imprese che ottengono certificazioni di sicurezza riconosciute a livello nazionale o internazionale, segno di impegno dell'impresa per la sicurezza e di volontà nell'aumentare la fiducia dei clienti e dei partner commerciali. Dall'altra parte, sarebbe corretto introdurre sanzioni per le imprese che non adottano misure di sicurezza adeguate alla loro attività in modo da incentivare le imprese a prendere seriamente la sicurezza informatica. Viste le frequenti e numerose violazioni informatiche

subite dalle imprese, avere una copertura assicurativa verso questi rischi può essere una soluzione utile. E quindi, si potrebbe favorire lo sviluppo di mercati assicurativi per la cybersecurity cosicché le imprese che adottano misure di sicurezza più rigorose potrebbero beneficiare di premi assicurativi più bassi, incoraggiando così gli investimenti nella sicurezza informatica. Nel presente studio sono state trattate le imprese del settore privato ma è essenziale favorire la collaborazione con il settore pubblico per sviluppare politiche di cybersecurity efficaci, per una migliore comprensione delle minacce e delle sfide, nonché a soluzioni più innovative. Implementando una combinazione di queste strategie, è possibile creare un ambiente favorevole che stimoli gli investimenti in cybersecurity da parte delle imprese, proteggendo così non solo le imprese stesse, ma anche i dati sensibili dei clienti e la sicurezza dell'intera comunità online.

Bibliografia

[1] Chang, F. R. (2012). Guest Editor's Column. *The Next Wave*, 19(4), 1–2

[2] ENISA (2015). "Definition of cybersecurity – gaps and overlaps in standardization". www.enisa.europa.eu/publications/definition-of-cybersecurity

[3] Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), 8

[4] The White House. (2009). Presidential Proclamation - National Cybersecurity Awareness Month. https://obamawhitehouse.archives.gov/the-press-office/presidential-proclamation-national-cybersecurity-awareness-month

[5] https://www.oed.com/

[6] Public Safety Canada (2018). National Cyber Security Strategy. Canada's Vision for Security and Prosperity in the Digital Age. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf

[7] Deibert, R., & Rohozinski, R. (2010). Liberation vs. control: The future of cyberspace. *J. Democracy*, *21*, 43

[8] Financial Stability Board (FSB) (2023). "Cyber Lexicon", https://www.fsb.org/wp-content/uploads/P130423-3.pdf

[9] Buzan, B., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers

[10] Kemmerer, R. (2003). Cybersecurity. *Proceedings of the 25th IEEE International Conference on Software Engineering:* 705-715

[11] Lewis, J. A. (2006). Cybersecurity and critical infrastructure protection. *Center for Strategic and International Studies*, *9*

[12] Amoroso, E. (2006). *Cyber Security*. New Jersey: Silicon Press.

[13] ITU. (2009). *Overview of Cybersecurity. Recommendation ITU-T X.1205*. Geneva: International Telecommunication Union (ITU).

[14] Committee on National Security Systems (2015), CNSSI No. 4009, Committee on National Security Systems (CNSS) Glossary

[15] Public Safety Canada. (2012). *Terminology Bulletin 281: Emergency Management Vocabulary*. Ottawa: Translation Bureau, Government of Canada.

[16] Canongia, C. & Mandarino, R. (2014). Cybersecurity: The New Challenge of the Information Society. In *Crisis Management: Concepts, Methodologies, Tools, and Applications* (pp. 60-80). IGI Global.

[17] Oxford University Press. 2014. Oxford Online Dictionary. Oxford: Oxford University Press. October 1, 2014

[18] DHS. (2014). A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. October 1, 2014

[19] Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21

[20] Schiliro, F. (2023). Towards a Contemporary Definition of Cybersecurity. *ArXiv.Org*

[21] von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102

[22] von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, *26*(1), 2–9

[23] ISO (2012). ISO/IEC 27032:2012 (Information technology – Security techniques – Guidelines for Cybersecurity).

[24] ISO (2018). ISO/IEC 27000:2018 (Information technology — Security techniques — Information security management systems — Overview and vocabulary)

[25] ISO (2023). ISO/IEC 27032:2023 (Cybersecurity — Guidelines for Internet security)

[26] ISACA (2016). The ISACA CSx Cybersecurity Fundamentals Study Guide. *ISACA CSx Cybersecurity fundamentals*

[27] ISO (2013). ISO/IEC 27014:2013 (Information technology – Security techniques – Governance of Information Security)

[28] Anderson, J. P. (1972). Computer security planning study. *Air Force Electronic System Division*

[29] Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of the IEEE*, *63*(9), 1278–1308

[30] Steve Lipner and Ross Anderson. 2018. CIA history. Personal communication.

[31] Piva A. (2023). Osservatori Cyber Security & Data Protection. La sicurezza dei dati tra confidenzialità, disponibilità e integrità. *Cyber Security*. https://blog.osservatori.net/it_it/sicurezza-informatica-disponibilita-e-integrita-dei-dati

[32] Ham, J. V. D. (2021). Toward a better understanding of "cybersecurity". *Digital Threats: Research and Practice*, *2*(3), 1-3

[33] Barrett, M. (2018), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework

[34] IBM. https://www.ibm.com/topics/cyber-attack

[35] IBM. https://www.ibm.com/topics/cybersecurity

[36] Proofpoint Research. (2022). 2022 Ponemon Cost of Insider Threats Global Report. *Threat Report*

[37] Verizon. (2023). 2023 Data Breach Investigations Report. *Data Breach Investigations Report*

[38] Vienažindytė I. NordVPN. (2022). I principali tipi di attacchi informatici. *Attacchi e violazioni* https://nordvpn.com/it/blog/tipi-di-attacchi-informatici/

[39] Banca d'Italia, Bundesbank, D., Authority, F. C., Authority, P. R., & Treasury, U. S. (2021). *Proposal for a common categorisation of IT incidents* (No. 6). Bank of Italy, Directorate General for Markets and Payment System

[40] IBM. https://www.ibm.com/topics/threat-actor

[41] IBM. (2023). Cost of a Data Breach Report 2023. https://www.ibm.com/reports/data-breach

[42] Clusit. (2023). Rapporto Clusit 2023 sulla Sicurezza ICT in Italia. Security Summit. https://clusit.it/wp-content/uploads/download/Rapporto-Clusit-marzo-2023_web.pdf

[43] Next Move Strategy Consulting. (July 26, 2023). Size of cyber security market worldwide from 2021 to 2030 (in billion U.S. dollars) [Graph]. In Statista. Retrieved October 11, 2023, from https://www-statista-com.ezproxy.biblio.polito.it/statistics/1256346/worldwide-cyber-security-market-revenues/

[44] Gartner. (October 13, 2022). Information security spending worldwide from 2017 to 2023, by segment (in million U.S. dollars) [Graph]. In *Statista*. Retrieved October 11, 2023, from https://www-statista-com.ezproxy.biblio.polito.it/statistics/790834/spending-global-security-technology-and-services-market-by-segment/

[45] CompTIA. (November 1, 2022). Most important cybersecurity areas worldwide in 2022 with a forecast until 2023 [Graph]. In *Statista*. Retrieved October 11, 2023, from https://www-statista-com.ezproxy.biblio.polito.it/statistics/1292944/critical-cybersecurity-area-worldwide/

[46] https://www.vmware.com/it/topics/glossary/content/zero-trust.html

[47] ISC2. (October 18, 2022). Size of cybersecurity workforce worldwide in 2022, by country [Graph]. In *Statista*. Retrieved October 11, 2023, from https://www-statista-com.ezproxy.biblio.polito.it/statistics/1172449/worldwide-cybersecurity-workforce/

[48] Cybersecurity360, & Osservatori Digital Innovation. (February 23, 2023). Market size of the cybersecurity sector in Italy from 2016 to 2022 (in million euros) [Graph]. In *Statista*. Retrieved October 11, 2023, from https://www-statista-com.ezproxy.biblio.polito.it/statistics/1055616/cybersecurity-market-size-italy/

[49] Il Sole 24 Ore. (February 23, 2023). Investments in the cybersecurity market in Italy from 2018 to 2022 (in billion euros) [Graph]. In *Statista*. Retrieved October 11, 2023, from https://www-statista-com.ezproxy.biblio.polito.it/statistics/1311084/cybersecurity-market-investments-italy/

[50] Netti E. (2023). Cybersecurity, il mercato balza a 1,9 miliardi. Ma l'Italia rimane fanalino di coda. *Il Sole 24 Ore*. https://www.ilsole24ore.com/art/cybersecurity-mercato-balza-19-miliardi-italia-AEiqjkrC

[51] Osservatori Digital Innovation. (February 23, 2022). Cybersecurity budget plan in Italy between 2018 and 2022 [Graph]. In *Statista*. Retrieved October 11, 2023, from https://www-statista-com.ezproxy.biblio.polito.it/statistics/1202046/cybersecurity-budget-plan-italy/

[52] Ministero dell'Economia e delle Finanze. Il Piano Nazionale di Ripresa e Resilienza (PNRR). https://www.mef.gov.it/focus/Il-Piano-Nazionale-di-Ripresa-e-Resilienza-PNRR/

[53] Ministero delle Imprese e del Made in Italy. PNRR - Piano Nazionale di Ripresa e Resilienza. https://www.mimit.gov.it/it/pnrr/piano

[54] Italiadomani. Piano Nazionale di Ripresa e Resilienza. Cybersecurity. https://www.italiadomani.gov.it/it/Interventi/investimenti/cybersecurity-sicurezza-informatica.html

[55] Governo italiano, Piano nazionale di ripresa e resilienza "Italia domani", https://www.governo.it/sites/governo.it/files/PNRR.pdf

[56] Gazzetta Ufficiale della Repubblica Italiana, Decreto-Legge 14 giugno 2021, n. 82, Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale. https://www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/sg

[57] Agenzia per Cybersicurezza Nazionale. Strategia Nazionale di Cybersicurezza. https://www.acn.gov.it/strategia/strategia-nazionale-cybersicurezza

[58] Agenzia per la Cybersicurezza Nazionale. Piano di implementazione. Strategia nazionale di cybersicurezza 2022-2026. https://www.acn.gov.it/ACN_Implementazione.pdf

[59] Gazzetta Ufficiale della Repubblica Italiana, DPCM del 17 febbraio 2017, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali. https://www.gazzettaufficiale.it/eli/id/2017/04/13/17A02655/sg

[60] Gazzetta Ufficiale della Repubblica Italiana, Decreto legislativo 18 maggio 2018, n.65, Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg

[61] Gazzetta Ufficiale della Repubblica Italiana, Decreto-legge 21 settembre 2019, n.105, Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica. https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg

[62] Gazzetta Ufficiale della Repubblica Italiana, Decreto-legge 16 luglio 2020, n.76, Misure urgenti per la semplificazione e l'innovazione digitale. https://www.gazzettaufficiale.it/eli/id/2020/07/16/20G00096/sg

[63] Gazzetta Ufficiale della Repubblica Italiana, DPCM del 30 luglio 2020, n.131, Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133. https://www.gazzettaufficiale.it/eli/id/2020/10/21/20G00150/sg

[64] Dipartimento per la trasformazione digitale. Strategia Cloud Italia. Gli indirizzi strategici per la Pubblica Amministrazione. https://innovazione.gov.it/dipartimento/focus/strategia-cloud-italia/

[65] Gazzetta Ufficiale della Repubblica Italiana, Decreto legislativo 8 novembre 2021, n.207, Attuazione della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il Codice europeo delle comunicazioni elettroniche (rifusione). https://www.gazzettaufficiale.it/eli/id/2021/12/09/21G00230/sg

[66] Gazzetta Ufficiale della Repubblica Italiana, Decreto-legge 21 marzo 2022, n.21, Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina. https://www.gazzettaufficiale.it/eli/id/2022/03/21/22G00032/SG

[67] Gazzetta Ufficiale della Repubblica Italiana, Decreto-legge 18 maggio 2022, n.92, Regolamento in materia di accreditamento dei laboratori di prova e di raccordi tra Centro di Valutazione e Certificazione Nazionale, i laboratori di prova accreditati e i Centri di Valutazione del Ministero dell'interno e del Ministero della difesa, ai sensi dell'articolo 1, comma 7, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133. https://www.gazzettaufficiale.it/eli/id/2022/07/15/22G00099/sg

[68] Gazzetta Ufficiale della Repubblica Italiana, DPCM del 15 giugno 2022, Definizione dei termini e delle modalità del trasferimento di funzioni, beni strumentali e documentazione dal Ministero dello sviluppo economico all'Agenzia per la cybersicurezza nazionale. https://www.gazzettaufficiale.it/eli/id/2022/06/30/22A03773/sg

[69] Gazzetta Ufficiale della Repubblica Italiana, DPCM del 1° settembre 2022, n.189, Regolamento recante disciplina dei meccanismi di raccordo tra obbligo di notifica e procedure di gara e delle misure di semplificazione delle modalità di notifica, dei termini e delle procedure relative all'istruttoria dei procedimenti rientranti nell'ambito di applicazione del decreto-legge 15 marzo 2012, n. 21, e successive modificazioni ed integrazioni, nel caso di affidamento di concessioni, anche di competenza regionale. https://www.gazzettaufficiale.it/eli/id/2022/12/06/22G00196/sg

[70] Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, *5*(4), 438-457

[71] Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in cybersecurity: Insights from the Gordon-Loeb model. *Journal of Information Security*, *7*(02), 49-59

[72] Wang, S. (2017). Optimal level and allocation of cybersecurity spending: Model and formula. *Available at SSRN 3010029*

[73] Hausken, K. (2006). Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers*, *8*, 338-349

[74] Willemson, J. (2006). On the Gordon & Loeb model for information security investment. *Proceedings of theWorkshop on the Economics of Information Security (WEIS).*

[75] Baryshnikov, Y. (2012, June). IT Security Investment and Gordon-Loeb's 1/e Rule. *Proceedings of the Workshop on the Economics of Information Security (WEIS).*

[76] Lelarge, M. (2012). Coordination in network security games: a monotone comparative statics approach. *IEEE Journal on Selected Areas in Communications*, *30*(11), 2210-2219

[77] Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Information security expenditures and real options: A wait-and-see approach. *Computer Security Journal, 19(2).*

[78] Krutilla, K., Alexeev, A., Jardine, E., & Good, D. (2021). The benefits and costs of cybersecurity risk reduction: A dynamic extension of the Gordon and Loeb model. *Risk Analysis*, *41*(10), 1795-1808

[79] Rowe, B. R., & Gallaher, M. P. (2006). Private sector cyber security investment strategies: An empirical analysis. In *The fifth workshop on the economics of information security (WEIS06).*

[80] Kissoon, T. (2020). Optimum spending on cybersecurity measures. *Transforming Government: People, Process and Policy*, *14*(3), 417-431

[81] Moore, T., Dynes, S., & Chang, F. R. (2016). Identifying how firms manage cybersecurity investment. In *Workshop on the Economics of Information Security (WEIS)* (pp. 1-27).

[82] Fedele, A., & Roner, C. (2022). Dangerous games: A literature review on cybersecurity investments. *Journal of Economic Surveys*, *36*(1), 157-187

[83] Liao, C.-H., & Chen, C.-W. (2014). Network externality and incentive to invest in network security. *Economic Modelling, 36*, 398–404.

[84] Jianqiang, G., Shue, M., & Weijun, Z. (2015, July). Analyzing information security investment in networked supply chains. In *2015 International Conference on Logistics, Informatics and Service Sciences (LISS)* (pp. 1-5)

[85] Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2018). Empirical evidence on the determinants of cybersecurity investments in private sector firms. *Journal of Information Security*, *9*(2), 133-153

[86] De Arroyabe, I. F., Arranz, C. F., Arroyabe, M. F., & de Arroyabe, J. C. F. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Computers & Security*, *124*, 102954

[87] Duso, T., & Schiersch, A. (2022). Let's Switch to the Cloud: Cloud Adoption and Its Effect on IT Investment and Productivity. In *Policy File*. CESifo Group Munich

[88] Shaikh, F. A., & Siponen, M. (2023). Organizational Learning from Cybersecurity Performance: Effects on Cybersecurity Investment Decisions. *Information Systems Frontiers*, 1-12

[89] Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. *Journal of Risk and Insurance*, *89*(3), 725-763

[90] Biancotti, C. (2017). The price of cyber (in) security: evidence from the italian private sector. *Bank of Italy occasional paper*, (407)

[91] Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability*, *60*, 100989

[92] Caldarulo, M., Welch, E. W., & Feeney, M. K. (2022). Determinants of cyber-incidents among small and medium US cities. *Government Information Quarterly*, *39*(3), 101703

[93] Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), 121-135

[94] Biancotti, C. (2017). Cyber attacks: preliminary evidence from the Bank of Italy's business surveys. *Bank of Italy Occasional Paper*, (373)