POLITECNICO DI TORINO

Laurea Magistrale Ingegneria Gestionale

Politecnico di Torino

Cybersicurezza e Digitalizzazione in Italia: Un'Analisi dei Modelli Economici e dei Dati Empirici.

Relatore:
Prof. Carlo Cambini

Candidato:
Daniele Del Chicca

Anno accademico 2024-2025

Sommario

Nel contesto attuale di trasformazione digitale, in cui le imprese italiane devono proteggere una mole crescente di dati sensibili, la cybersicurezza assume un ruolo fondamentale. Questa tesi esplora i modelli economici che spiegano le decisioni aziendali sugli investimenti in sicurezza informatica. Attraverso una revisione della letteratura, si esaminano modelli basati sulla teoria dei giochi per comprendere come i fallimenti di mercato e le esternalità influenzino le decisioni strategiche delle imprese.

Successivamente, lo studio analizza i dati empirici sulla digitalizzazione e sulla cybersicurezza in Italia, utilizzando le informazioni del rapporto ISTAT "ICT nelle imprese". Viene proposta una classificazione dei settori economici italiani basata sulle interdipendenze emerse in letteratura, per analizzare come queste influenzino l'adozione di misure di sicurezza e l'incidenza degli attacchi informatici. L'analisi evidenzia le principali tendenze e sfide nei diversi settori economici, offrendo un quadro aggiornato delle pratiche di sicurezza adottate dalle imprese italiane. Questo lavoro contribuisce a chiarire il legame tra teoria economica e realtà empirica nel contesto italiano.

Indice

1 Introduzione

1.1 Digitalizzazione delle imprese

1.1.1 Le imprese prima della digitalizzazione

Non molto tempo fa, appena prima degli anni 70, quando non era ancora avvenuta la digitalizzazione come la conosciamo oggi, le aziende, erano comunque molto simili ad adesso come forma e struttura dei processi e delle funzioni che le componevano ma il modo di lavorare era molto diverso.

Tutto era in formato cartaceo, ogni cosa quindi era gestita manualmente, i documenti della azienda, come le comunicazioni o report o file di qualunque natura erano letteralmente dei fogli scritti a macchina in genere organizzati in fascicoli che poi venivano conservati in raccoglitori dentro a cassetti e armadi.

I calcoli per operazioni contabili o calcoli finanziari dovevano essere svolti a mano, necessitando di essere ricontrollati più e più volte, con comunque un elevato rischio di errore umano e lentezza delle operazioni.

Le comunicazioni all'interno della azienda erano gestite attraverso strumenti come i bollettini e le note passate tra i dipendenti con l'aiuto di assistenti che coordinavano gli scambi. Le riunioni si potevano svolgere solo di persona. Le comunicazioni all'esterno invece erano limitate, venivano utilizzati scambi via posta o telefonici.

Per quanto riguarda le comunicazioni con i clienti, questi venivano raggiunti sempre attraverso pubblicità, ma queste erano poste su volantini o brochure poi distribuite per le strade o tramite inserzioni sui giornali. Era molto difficile fare *targhettizzazioni* specifiche su alcuni tipi di clientela così come raccogliere feedback su quali campagne di marketing avessero dato i risultati migliori

In generale anche il processo decisionale era diverso. Il concetto di dato non era come lo intendiamo oggi, venivano registrate delle informazioni riguardo alle vendite e alla contabilità, anche dati riguardo i clienti, ma il recupero di informazioni specifiche dai registri cartacei era un processo lento e laborioso che necessitava di una precisa conoscenza di come le informazioni fossero organizzate rendendo difficile l'accesso e quasi impraticabile l'analisi in grandi quantità. Le imprese quindi si affidavano a metodi manuali per la creazione di report basandosi più che altro su campioni ridotti di dati piuttosto che analisi complete, limitando notevolmente la capacità di identificare tendenze portando a decisioni meno informate ed efficaci.

1.1.2 Evoluzione della tecnologia

Questo panorama negli ultimi decenni è stato completamente rivoluzionato grazie alla evoluzione tecnologica.

L'introduzione dei personal computers negli anni 80 ha segnato un primo punto di svolta fondamentale, spostando il paradigma lavorativo dal manuale al digitale. Questo ha permesso di semplificare numerosi processi che prima richiedevano un notevole dispendio di tempo e risorse umane.

L'utilizzo di appositi software ha reso possibile scrivere, ma anche modificare e aggiornare facilmente documenti di testo applicando diverse formattazioni. Questi poi potevano essere stampati o condivisi attraverso la rete e in fine archiviati digitalmente senza occupare spazio fisico.

Il passaggio a fogli di calcolo elettronici ha permesso di svolgere operazioni complesse in modo automatico minimizzando gli errori umani, ma ha anche dato la possibilità di generare report dettagliati con grafici dinamici con pochi clic del mouse migliorando la capacità di analizzare e veicolare contenuti.

In generale tutte le informazioni che prima erano cartacee, sono diventate digitali, dei bit salvati su un computer, in questo modo gli hard disk hanno del tutto sostituito i metodi di archiviazione fisici permettendo di risparmiare spazio fornendo una maggiore protezione da danni accidentali ai i file.

Con il secondo grande punto di svolta tecnologico poi: l'introduzione di internet negli anni 2000 ha ulteriormente rivoluzionato il panorama. La comunicazione sia interna che esterna è cambiata con strumenti come le mail in grado spedire i documenti elettronici ovunque nel mondo in pochi instanti arrivando fino al telelavoro che oggi svincola quasi del tutto dalla presenza fisica in ufficio. Si è poi sviluppato il cloud computing che in fine ha portato l'archiviazione e la gestione dei dati ancora ad un livello superiore permettendo di salvare i file direttamente nel "cloud" ossia server dislocati nel mondo non direttamente di proprietà della azienda, rendendo le informazioni accessibili da tutto il mondo svincolando ulteriormente da spazi fisici.

1.1.3 Vantaggi della digitalizzazione

L'implementazionie di questi nuovi strumenti, dai computer ai software a internet, nella routine aziendale ha portato con se fin da subito evidenti vantaggi che hanno contribuito a renderli uno standard nel mondo del lavoro

Primo fra tutti ovviamente la velocità ed efficienza che deriva dalla automazione di molti processi, aumentando cosi anche la produttività ottimizzando i flussi di lavoro.

Ma i vantaggi più significativi, non sono derivati dal miglioramento di processi esistenti, bensì sono emersi dai nuovi processi che la digitalizzazione ha permesso di sviluppare. La trasformazione di ogni informazione precedentemente cartacea in un dato digitale salvato su internet ha permesso una raccolta, e gestione delle informazioni mai vista prima d'ora. I computer e in generale la connessione ad internet infatti, non ha toccato solo le aziende bensì hanno raggiunto ogni ambiente anche non lavorativo. Dai dispositivi personali come cellulari o orologi smart o elettrodomestici connessi alla rete, tutto oggi in quasi ogni ambito è diventato in grado di generare infomazioni e di salvarle su un server dove possono essere accessibili. Questa nuova accessibilità a quantità di informazioni cosi grandi ha spinto verso lo sviluppo della disciplina della analisi dei dati arrivando al moderno concetto di "Big data analysis". Riuscendo a tenere traccia di quasi ogni cosa, da aspetti riguardanti i processi interni a informazoni di ogni genere sui propri clienti, le aziende di oggi sono diventate in grado di accedere ad una conoscienza motlo più apprfondita di fenomeni in tutti gli aspetti del business permettendo così di prendere decisioni in modo molto più informato e consapevole.

Un esempio lampante di questo lo si ha in ambito produttivo pensando alla industria 4.0 e l'IOT: l'evoluzione delle tecnologie dei macchinari che compongono gli impianti è progredita al punto di poter connettere ad internet molti dei singoli elementi, rendendoli in grado di rilevare e trasmettere il loro stato, che poi viene salvato ed archiviato. In questo modo, per ogni componente si rendono disponibili serie storiche dettagliate del loro stato operativo, con una precisione che può arrivare al secondo o persino al millisecondo. Queste informazioni, se aggregate e analizzate con tecniche adeguate, possono fornire stime sull'usura dei macchinari. Tali dati sono utili per valutare investimenti e prevedere rotture future di alcuni pezzi, permettendo di programmare con anticipo le manutenzioni. Questo aiuta a risparmiare notevoli somme di denaro, evitando fermi imprevisti delle linee produttive. Inoltre, queste informazioni offrono una visione completa della produttività dell'impianto, facilitando decisioni strategiche per migliorare le performance complessive.

Un altro esempio invece riguarda i consumatori ossia i clienti delle aziende, negli ultimi decenni il digitale non ha rivoluzionato solo il modo di gestire l'impresa ma anche la vita quotidiana delle persone. Con i computers, telefoni e molti altri dispositivi smart connessi ad internet le persone hanno incominciato ad esplorare le infinite risorse del web, che vanno dagli e-commerce ai social media, fino all'intrattenimento digitale e molto altro ancora. Questo costante utilizzo della rete ha permesso alle aziende di raccogliere una vasta quantità di dati sui comportamenti dei consumatori, consentendo loro di analizzarli e di comprendere meglio il proprio pubblico di riferimento.

1.1.4 Svantaggi della digitalizzazione

Le nuove tecnologie hanno quindi indubbiamente apportato numerosi vantaggi, alcuni dei quali del tutto inaspettati, ma hanno anche introdotto altrettanto imprevedibili sfide.

In particolare una delle complicazioni più grandi con cui le imprese si devono confrontare oggi è la cybersicurezza. Internet, con la sua straordinaria capacità di interconnettere dispositivi e persone, ha reso possibile salvare, trasmettere e reperire informazioni da qualsiasi luogo. Questa stessa facilità di accesso, che ha rivoluzionato la gestione e l'analisi dei dati aziendali, ha però anche aperto la porta a utilizzi impropri. Criminali informatici sfruttano questa interconnessione per accedere indebitamente a dati sensibili raccolti dalle aziende. Le imprese si trovano così esposte a rischi che vanno dal furto di informazioni confidenziali alla compromissione dei loro sistemi operativi, situazioni che possono avere gravi ripercussioni sulla loro operatività e sulla fiducia dei loro clienti.

Le principali minacce derivanti da attacchi informatici oggi si dividono in tre categorie:

Furto di dati sensibili

In queste occasioni i cosiddetti hackers riescono ad introdursi nella rete aziendale e rubare dati delle aziende che possono andare dalle enormi quantità di informazioni raccolte sui clienti o dati riguardanti le attività operative o anche semplicemente documenti privati dell'impresa. Riguardo al furto di informazioni sui clienti un caso storico di spicco è sicuramente quello di Yahoo (2013-2014): Yahoo ha subito due massicci attacchi informatici che hanno coinvolto i dati di 3 miliardi di account degli utenti. Le informazioni rubate includevano nomi, indirizzi email, date di nascita, domande e risposte di sicurezza crittografate e non. Attacchi di questo tipo sono spesso pericolosi perché minano pesantemente il rapporto di fiducia tra l'impresa e i propri clienti i quali vedendo i propri dati pubblicati illegalemnte a causa di una scarsa sicurezza informazica dell'azienda fornitrice del servizio possono decidere di passare ad uno dei competitors.

Riguardo invece alla divulgazione di informazioni sensibili per la azienda stessa, un altro caso importante di violazione è stato quello Sony Pictures Entertainment (2014): durante questo noto attacco informatico, una grande quantità di dati confidenziali è stata esposta, incluse e-mail tra dirigenti, informazioni sui salari dei dipendenti, dettagli di progetti futuri non ancora annunciati e copioni di film inediti. L'attacco in questione ha di fatto avuto enormi ripercussioni sule strategie aziendali.

Distruzione di dati sensibili

Un altro esempio notevole è stato l'attacco ransomware WannaCry del 2017, che ha colpito migliaia di organizzazioni in tutto il mondo, inclusi ospedali, istituti governativi e aziende.

WannaCry era un malware che sfruttava una vulnerabilità nel sistema operativo Windows, specificamente nel protocollo di condivisione file Server Message Block (SMB). Una volta infettato un sistema, il malware crittografava i file presenti sul computer, rendendoli inaccessibili agli utenti, e quindi richiedeva un pagamento in Bitcoin per fornire la chiave di decrittazione.

L'attacco WannaCry ha avuto un impatto significativo su molte organizzazioni, causando la perdita di dati sensibili e interrompendo le operazioni commerciali. In particolare, nel Regno Unito, il National Health Service (NHS) è stato gravemente colpito, con molti ospedali che hanno dovuto sospendere le operazioni non critiche a causa dell'impossibilità di accedere ai dati dei pazienti.

Questo attacco ha evidenziato la vulnerabilità delle organizzazioni alle minacce informatiche e ha sottolineato l'importanza di mantenere aggiornati i sistemi e di adottare misure di sicurezza informatica robuste per proteggere i dati sensibili.

Stop delle funzioni produttive della azienda

Un esempio eclatante potrebbe essere l'attacco informatico contro la centrale nucleare di Natanz in Iran nel 2010. In questo attacco, il malware noto come Stuxnet è stato utilizzato per compromettere i sistemi di controllo industriale della centrale, causando malfunzionamenti e danni alle centrifughe utilizzati per l'arricchimento dell'uranio.

Stuxnet è stato progettato per infiltrarsi nei sistemi informatici delle centrifughe, modificare il loro funzionamento e causare danni fisici. Questo attacco ha avuto un impatto diretto sul programma nucleare iraniano, rallentando i progressi dell'arricchimento dell'uranio e creando problemi operativi significativi nella centrale nucleare.

1.1.5 Entità del problema

Appurato che i dati digitalizzati sono quindi soggetti ad attacchi informatici in grado di nuocere gravemente alle imprese, quanto è effettivamente frequente questo fenomeno nel mondo, in particolare in Europa e in Italia? Costituisce effettivamente un problema rilevante per le imprese di oggi?

Trend mondiali

Secondo le ricerche di Cybersecurity Ventures, si stima che il cybercrime nel 2024 costerà al mondo più di 9,5 trilioni di dollari, posizionandolo come la terza economia globale, dietro solo a Stati Uniti e Cina.

I costi associati agli attacchi informatici sono previsti in aumento del 15% annuo, raggiungendo i 10,5 trilioni di dollari all'anno entro il 2025. Questo aumento riflette l'escalation sia nella frequenza che nella crescente sofisticazione degli attacchi che le imprese subiscono. Il costo medio di una violazione dei dati, secondo uno studio dell'IBM ha raggiunto ormai i 4,45 milioni di dollari nel 2023, con un incremento del 2,3% rispetto al 2022. Dal 2020, il costo medio è aumentato del 15,3%. La grande maggioranza delle violazioni (82%) ha interessato dati archiviati nel cloud, con il 39% delle violazioni che ha coinvolto più ambienti. Questi dati suggeriscono che non solo la frequenza, ma anche i costi delle violazioni stanno crescendo esponenzialmente.

Impatto a livello geografico e settoriale

Secondo lo stesso studio di IBM, le cinque zone del mondo con il costo medio più elevato per ogni violazione dei dati (aggiornato a marzo 2023) sono le seguenti:
Gli Stati Uniti si collocano al primo posto per il tredicesimo anno consecutivo, con un costo medio di 9,48 milioni di dollari per violazione, registrando un incremento dello 0,4% rispetto all'anno precedente.
Segue il Medio Oriente, al secondo posto, con un costo di 8,07 milioni di dollari, aumentato di oltre 600.000 dollari (+8,2%) rispetto all'anno precedente.
Il Canada si posiziona terzo con 5,31 milioni di dollari. La Germania, con 4,67 milioni di dollari, e il Giappone, con 4,52 milioni di dollari, completano la lista dei primi cinque.

I cinque settori più colpiti da violazioni di dati invece includono: in cima alla lista il settore sanitario, che continua a registrare i costi più elevati per violazione dei dati rispetto a tutti gli altri settori, con un aumento da 10,10 milioni di dollari nel 2022 a 10,93 milioni di dollari nel 2023, ovvero un incremento dell'8,2%.

Negli ultimi tre anni, il costo medio di una violazione nel settore sanitario è salito del 53,3%, con un incremento di oltre 3 milioni di dollari rispetto ai 7,13 milioni di dollari del 2020. Questo ambito, soggetto a rigide regolamentazioni, è ritenuto infatti dal governo statunitense un'infrastruttura critica. Dall'inizio della pandemia di COVID-19, ha evidenziato costi medi per violazione sensibilmente superiori.

Al secondo posto si posiziona il settore finanziario, con un costo medio di 5,90 milioni di dollari, seguito dall'industria farmaceutica, che registra 5,01 milioni di dollari per violazione.

Chiudono la classifica il settore energetico al quarto posto, che guadagna una posizione rispetto all'anno precedente, e l'industria manifatturiera, che sostituisce il tecnologico del 2022 con un aumento del 5,8%.

Il tipo più comune di dati rubati o compromessi è stato il Customer Personal Identifiable Information – PII (IBM Cost of a Data Breach Report 2023) – I primi cinque tipi di dati che sono stati rubati o compromessi nel 2023 sono stati:

- PII del cliente
- PII dei dipendenti
- Proprietà intellettuale (PI)
- Dati dei clienti (non PII)
- Dati societari

Impatto a livello Italiano

Arrivando all' Italia invece, nonostante non emerga tra i primi posti nelle classifiche globali per i costi medi per violazione secondo IBM—dove si posiziona nona con un valore di 3,86 milioni di dollari, inferiore di quasi un milione alla media mondiale, ma con un incremento di quasi 130.000 dollari rispetto al 2022—la situazione dei cyber attacchi è particolarmente critica.

Secondo uno studio di Trend Micro, basato sul rapporto del Clusit 2024, l'Italia si conferma per il terzo anno consecutivo come il paese più colpito da cyber attacchi (in termini di numero e gravità) in Europa e il quarto a livello mondiale, dopo Stati Uniti, Giappone e India con il settore sanitario, bancario e manifatturiero tra i settori più colpiti.

Nel 2023 sul territorio nazionale italiano sono stati registrati più di 277.616.731 di malware intercettati, in forte aumento rispetto ai 246.941.068 del 2022.
Su 2.779 incidenti gravi avvenuti nel mondo, ossia violazioni che comportano una notevole perdita di dati personali o aziendali, interruzioni dell'attività commerciale, o danni significativi alla reputazione delle imprese coinvolte, più di 310 sono avvenuti in Italia.
Ciò che sorprende di più però è il fatto che continui a crescere l'incidenza degli attacchi rivolti a organizzazioni italiane rispetto al totale nel mondo, nel 2022 gli attacchi in Italia erano il 7,6% del campione complessivo, mentre nel 2023 la quota sale all'11,2%, con un trend che continua a crescere.

In sintesi, il problema della cybersicurezza è più reale che mai, specialmente nel nostro paese dove le imprese più colpite sono le piccole e medie (con un incremento dell'85% degli attacchi solo nel 2023) una tendenza preoccupante data la loro cruciale importanza nell'economia nazionale.

1.1.6 Investimenti in cybersicurezza

Nonostante gli attacchi informatici non siano solo un fenomeno diffuso, ma anche in rapida crescita, le aziende non sono completamente indifese di fronte a queste minacce. Esistono, infatti, numerosi metodi, strategie e tecnologie altamente efficaci per contrastarli, tutti racchiusi nel termine "cybersicurezza". Questo campo comprende una vasta gamma di soluzioni progettate per proteggere le infrastrutture informatiche, difendere i dati sensibili e assicurare la continuità operativa delle imprese. Con il costante sviluppo di nuove tecnologie di sicurezza e l'aggiornamento delle pratiche di difesa, la cybersicurezza si è affermata come una componente essenziale nella strategia complessiva delle organizzazioni per fronteggiare i rischi sempre più sofisticati nel panorama informatico contemporaneo.

Metodi e Strategie di Cybersicurezza

La cybersicurezza sfrutta un'ampia varietà di tecnologie avanzate e pratiche consolidate per salvaguardare reti, computer, software e dati. Le strategie più efficaci adottate dalle aziende per contrastare le minacce informatiche includono:

1. **Protezione dei dati:** L'adozione di tecnologie come la crittografia e il backup regolare è fondamentale per proteggere le informazioni aziendali da perdite e furti. La crittografia trasforma i dati sensibili in codici indecifrabili per chi non possiede la chiave necessaria alla loro lettura, offrendo un livello di sicurezza vitale durante la trasmissione e l'archiviazione dei dati. I backup regolari garantiscono che, anche in caso di attacco informatico o guasto tecnico, le informazioni aziendali possano essere rapidamente ripristinate da una copia sicura.

2. **Sicurezza delle reti:** L'utilizzo di firewall robusti e avanzati sistemi di rilevamento delle intrusioni aiuta a prevenire accessi non autorizzati alle reti aziendali. I firewall agiscono come barriere che filtrano il traffico di rete per bloccare gli accessi indesiderati, mentre i sistemi di rilevamento delle intrusioni monitorano continuamente la rete per identificare e reagire a tentativi sospetti di intrusione.

3. **Sicurezza delle applicazioni:** Integrare misure di sicurezza già nella fase di progettazione del software è essenziale per prevenire vulnerabilità future. Questo approccio, noto come "security by design", assicura che le applicazioni siano protette da attacchi informatici sin dal loro sviluppo, riducendo il rischio di exploit.

4. **Formazione degli utenti:** Programmi di educazione continua sono essenziali per sensibilizzare i dipendenti sui rischi di sicurezza e sulle migliori pratiche per evitarli. La formazione dovrebbe coprire argomenti come il riconoscimento e la gestione di email di phishing, l'importanza di password forti e l'utilizzo sicuro di reti e dispositivi.

L'implementazione di queste strategie richiede un impegno costante e una valutazione periodica per adattarsi alle nuove minacce che emergono costantemente nel

panorama della sicurezza informatica. Un approccio multilivello alla cybersicurezza non solo aumenta la resilienza delle aziende contro gli attacchi, ma contribuisce anche a costruire una cultura della sicurezza che permea tutte le attività aziendali.

Investimenti in Cybersicurezza

L'implementazione delle strategie di cybersicurezza descritte non è priva di costi significativi. Proteggere reti, dati e infrastrutture informatiche richiede un investimento continuo e spesso elevato in tecnologie avanzate e formazione del personale. L'adozione di soluzioni come la crittografia, i firewall avanzati, e i programmi di formazione continua comporta non solo l'acquisto di tecnologia ma anche la gestione e l'aggiornamento costante di queste risorse per tenere il passo con le minacce in evoluzione.

A livello globale, gli investimenti in cybersicurezza hanno mostrato una crescita esponenziale. Le spese nel settore della sicurezza informatica sono stimate aver raggiunto circa 200 miliardi di dollari nel 2023, con previsioni che indicano una crescita sostenuta negli anni a venire. In Europa, le cifre si aggirano intorno ai 40 miliardi di dollari, riflettendo l'importanza crescente che il continente attribuisce alla protezione contro gli attacchi informatici. In Italia, gli investimenti continuano ad aumentare, superando i 2 miliardi di dollari, segno dell'urgenza percepita dalle aziende e dalle istituzioni di rafforzare le proprie difese digitali.

Questi investimenti significativi sono essenziali per mitigare i rischi associati al cybercrime e per garantire la continuità operativa delle aziende in un ambiente sempre più digitalizzato e interconnesso. La cybersicurezza, quindi, non è solo una necessità operativa ma un investimento strategico che protegge i valori fondamentali dell'impresa e sostiene la fiducia di clienti e partner.

Fallimenti di Mercato nell'Investimento in Cybersicurezza

Come tutti gli investimenti, anche quelli in cybersicurezza, che ammontano a cifre considerevoli, sono soggetti a inefficienze causate da fallimenti di mercato. Questi fallimenti spesso rendono gli investimenti meno efficaci in certi contesti o troppo ingenti in altri, influenzati dalla struttura specifica di ciascun mercato. La natura e l'entità di questi fallimenti di mercato dipendono strettamente dalla struttura del mercato stesso, generando diverse tipologie di inefficienze. In ambienti dove le reti sono condivise o i dati sono interdipendenti, può verificarsi il fenomeno del free riding, dove le aziende si affidano sulla sicurezza fornita da altri senza investire a sufficienza. Questo comportamento tende a mantenere l'investimento complessivo in sicurezza al di sotto del livello ottimale. Al contrario, in settori dove per esempio un attacco può offrire vantaggi competitivi indiretti — come il "business stealing" quando un concorrente subisce una violazione dati — le aziende possono essere indotte a sovrainvestire in cybersicurezza per proteggersi da queste potenziali minacce, portando a investimenti eccessivi rispetto al beneficio effettivo.

Nel prossimo capitolo verranno illustrati gli studi accademici e di settore che esplorano come vari fattori di mercato influenzano gli investimenti e verranno analizzate le strategie per ottimizzare le risorse e migliorare la sicurezza complessiva.

2 Literature Review

2.1 Introduzione alla letterature:

2.1.1 Gli Investimenti e il Livello Ottimo Sociale

Un investimento ottimo si verifica quando le risorse sono allocate in modo tale da massimizzare il benessere complessivo della società, tenendo conto sia dei benefici che dei costi associati. Questo concetto è spesso analizzato attraverso il prisma dell'efficienza paretiana, dove un'allocazione è considerata ottimale se non è possibile migliorare la situazione di un individuo senza peggiorare quella di un altro.

Per determinare il livello ottimale di investimento, è necessario considerare i benefici marginali e i costi marginali associati all'investimento. L'investimento ottimo si raggiunge quando il beneficio marginale netto per la società di una unità aggiuntiva di investimento è uguale al costo marginale netto. In termini analitici, questo implica che la funzione di utilità sociale è massimizzata quando la derivata del beneficio sociale totale rispetto all'investimento è uguale alla derivata del costo sociale totale.

Nel contesto della cybersecurity, un investimento ottimo sarebbe quello in cui le risorse dedicate alla protezione dei sistemi informatici e dei dati riducono al minimo il rischio di cyberattacchi, mantenendo i costi di implementazione entro limiti sostenibili. I benefici includono la protezione contro le perdite finanziarie, la salvaguardia della privacy degli utenti e il mantenimento della fiducia nei sistemi digitali, mentre i costi comprendono l'implementazione, la manutenzione e l'aggiornamento continuo delle misure di sicurezza.

Nella pratica, gli investimenti spesso si discostano dall'ottimo sociale a causa di una serie di fattori, tra cui le esternalità. Le esternalità sono effetti collaterali delle decisioni economiche che non sono completamente internalizzati dai decisori, influenzando il livello di investimento effettivo rispetto a quello ottimale.

2.1.2 Esternalità Positive

Le esternalità positive si verificano quando un investimento genera benefici che non sono interamente captati dall'investitore. Per esempio, un'azienda che investe in robuste misure di sicurezza informatica non solo protegge se stessa, ma anche altre aziende e individui che interagiscono con essa. Tuttavia, poiché l'azienda non può catturare completamente questi benefici esterni, potrebbe essere riluttante a investire al livello ottimale dal punto di vista sociale, lasciando quindi gli utenti scoperti, rendendoli suscettibili di cyberattacchi che altrimenti avrebbero potrebbero potuto essere prevenuti se ogni attore avesse investito adeguatamente.

2.1.3 Esternalità Negative

Le esternalità negative si verificano quando le decisioni di un individuo o di un'impresa impongono costi su altre parti che non sono coinvolte nella decisione. Questi costi aggiuntivi non sono riflessi nei costi privati dell'attore decisionale, ma sono subiti dalla società nel suo complesso. Nel contesto della cybersecurity, ad esempio, un'azienda che non investe adeguatamente nella propria sicurezza informatica può aumentare il rischio di cyberattacchi per altre aziende e utenti collegati, generando vulnerabilità sistemiche che potrebbero essere evitate con investimenti coordinati e sufficienti. Di conseguenza, gli utenti e le altre aziende rimangono esposti a rischi informatici che avrebbero potrebbero potuto essere prevenuti.

2.1.4 Il Ruolo della Teoria dei Giochi

La teoria dei giochi offre un potente strumento analitico per comprendere e analizzare gli scostamenti dagli investimenti ottimali a causa delle esternalità. Questa disciplina studia le interazioni strategiche tra diversi attori economici, modellando le loro decisioni come giochi in cui ogni partecipante cerca di massimizzare il proprio payoff, tenendo conto delle possibili azioni degli altri.

Analisi delle Interazioni Strategiche

Utilizzando i concetti di equilibrio di Nash, la teoria dei giochi può aiutare a identificare gli esiti in cui tutti gli attori agiscono in modo razionale dato il comportamento degli altri. Tuttavia, questi equilibri non sempre coincidono con l'ottimo sociale, poiché ogni attore tende a considerare solo i propri benefici e costi privati, ignorando le esternalità. Ad esempio, in un gioco di cybersecurity, ogni azienda può scegliere il livello di investimento che minimizza i propri costi, anche se questo porta a un livello complessivo di sicurezza inferiore all'ottimo sociale.

2.1.5 Conclusione

In conclusione, mentre l'ottimo sociale degli investimenti rappresenta un obiettivo auspicabile, nella pratica spesso ci si discosta da questo livello ideale a causa delle esternalità e delle interazioni strategiche tra gli attori economici. La teoria dei giochi fornisce strumenti essenziali per analizzare e comprendere questi scostamenti,

offrendo un quadro matematico per valutare come le decisioni individuali possano divergere dall'interesse collettivo. Attraverso una migliore comprensione delle dinamiche di gioco, è possibile progettare interventi che incentivino gli investimenti necessari per massimizzare il benessere collettivo, affrontando al contempo le sfide.

2.2 Suddivisione della letteratura

La letteratura relativa agli investimenti in cybersicurezza e al loro impatto sul benessere sociale è vasta e complessa, articolandosi in vari filoni di studio che esplorano diversi aspetti di questo tema. Per una comprensione completa e dettagliata, possiamo suddividere la letteratura nei seguenti capitoli principali:

2.2.1 No interdipendenze

In questo primo filone, il più semplice, originato da Gordon e Loeb (2002) si analizzano gli incentivi ad investire escludendo per assunzione ogni forma di interdipendenza. In questo modo viene considerata una sola impresa intenta a decidere il livello ottimale di investimento in contromisure di cybersicurezza per proteggere un set di informazioni da eventuali attacchi.

2.2.2 Interdipendenza tecnica

Sulla base del contributo di Kunreuther e Heal (2003) e Varian (2004), è emerso un secondo filone di ricerca che esplora per primo le interdipendenze relative alla sicurezza. In particolare questa letteratura si concentra sui contesti in cui più imprese che non competono sul mercato dei prodotti, devono decidere simultaneamente il livello di investimento in cybersicurezza che vogliono effettuare, tenendo però conto che operando il loro business tramite una rete informatica comune. In questo modo viene introdotto il concetto di spillover tecnico ossia una esternalità positiva tale per cui tutti beneficiano dell'investimento di tutti coloro che fanno parte dello stesso network esplorando così gli effetti del free riding in questo contesto.

2.2.3 Interdipendenza di mercato

Un terzo filone della letteratura, avviato da Garcia e Horowitz (2007), esamina le scelte di investimento in cybersicurezza delle imprese che sono concorrenti nel mercato dei prodotti ma che operano utilizzando sistemi informatici non interconnessi. In questo contesto, gli investimenti in cybersicurezza di ciascuna impresa non influenzano il livello di protezione delle altre, poiché i sistemi informatici separati impediscono qualsiasi forma di spillover tecnico. Questo approccio analizza come le imprese decidono autonomamente il livello ottimale di investimento in cybersicurezza, considerando solo i benefici diretti per sé stesse senza poter contare su vantaggi derivanti dagli investimenti dei concorrenti.

2.2.4 Interdipendenza tecnica e di mercato

In questo quarto filone, vengono esaminati i casi in cui si verificano contemporaneamente sia le interdipendenze tecniche che quelle di mercato. Questo contesto coinvolge imprese che sono concorrenti nel mercato dei prodotti finiti e che utilizzano lo stesso network informatico comune, portando così alla compresenza di entrambe le forme di spillover. Le imprese devono affrontare sia le esternalità positive degli investimenti in cybersicurezza nella rete comune (spillover tecnici), sia la

competizione diretta sul mercato dei prodotti (spillover di mercato). Questo scenario complesso influenza significativamente le strategie di investimento, introducendo nuove dinamiche di cooperazione e competizione tra le imprese.

2.2.5 Altri Contributi

Infine, verranno analizzati anche altri contributi che non rientrano strettamente nella classificazione appena descritta, ma che offrono ulteriori prospettive e approfondimenti sul tema della cybersicurezza e degli investimenti aziendali.

2.3 No interdipendenze

La letteratura sugli investimenti in cybersicurezza senza forme di interdipendenze costituisce una delle prime e fondamentali aree di studio nel campo della sicurezza informatica. Questo filone di ricerca si concentra sul modo in cui le singole imprese decidono autonomamente il livello ottimale di misure in cybersicurezza, senza considerare le influenze o gli effetti delle decisioni di altre imprese.

I primi studi in questo ambito si focalizzano su modelli teorici che analizzano il comportamento delle imprese in un contesto isolato. L'obiettivo principale è determinare il livello ottimale di investimento in cybersicurezza per minimizzare i rischi associati agli attacchi informatici, tenendo conto dei costi degli investimenti e dei benefici derivanti dalla protezione delle informazioni.

Questa parte della letteratura si differenzia nettamente dagli studi successivi sugli spillover tecnici e di mercato in quanto mentre le ricerche sugli spillover si occupano di come le decisioni di cybersicurezza di una singola impresa possano avere effetti positivi o negativi su altre imprese, gli studi iniziali senza interdipendenze trattano le imprese come entità indipendenti, il cui comportamento non influisce né è influenzato da altre imprese.

In questo contesto il modello di Gordon e Loeb (2002) è uno dei primi contributi più significativi. Esso fornisce un quadro teorico per comprendere come una singola impresa possa determinare il livello ottimale di investimento in cybersicurezza, focalizzandosi esclusivamente sui propri rischi e benefici. Questo modello è diventato un punto di riferimento essenziale, non solo per la sua semplicità e applicabilità, ma anche perché ha gettato le basi per ulteriori studi che esplorano le dinamiche più complesse delle interdipendenze tra imprese. Per questi motivi adesso andremo ad analizzare nel dettaglio questo modello.

2.3.1 Il modello

Il modello matematico di Gordon e Loeb rappresenta il quadro più semplice per studiare i trade-off economici legati agli investimenti in cyber sicurezza ed è costituito da un modello mono-periodale a un solo decisore (una sola impresa). Come detto in precedenza, le interazioni con altre imprese sono escluse per assunzione, di conseguenza le decisioni dell'impresa non sono influenzate da fattori esterni. L'impresa in questione è caratterizzata da neutralità al rischio e deve decidere quanto investire per proteggere un set di informazioni.

In questo contesto denotiamo con

- X il valore delle informazioni dell'impresa definite come i suoi ricavi.
- $t \in [0, 1]$ la probabilità di subire un attacco informatico, che per semplicità, ma senza perdita di generalità, consideriamo $= 1$.
- $v \in [0, 1]$ la probabilità di successo dell'attacco prima che l'investimento per migliorare le difese sia stato effettuato (condizionata quindi all'avvenimento dell'attacco).
- $a \cdot X$, $a \in [0, 1]$ la perdita monetaria dovuta all'attacco in caso si verificasse.

L'impresa deve quindi decidere il livello di investimento monetario $I \geq 0$ per ridurre la probabilità di successo dell'attacco v.

La probabilità post investimento di successo dell'attacco informatico è data dalla funzione $\pi(I, V) \in [0, v]$ ed è caratterizzata dalle seguenti assunzioni:

- **A1:** $\pi(I, 0) = 0$
  Questo vuol dire che un set di informazioni non vulnerabile resterà perfettamente protetto a prescindere dal livello di investimento, anche se 0.
- **A2:** $\pi(0, v) = v$
  Questo significa che, se non si effettuano investimenti, la probabilità di successo di un attacco rimane pari alla vulnerabilità intrinseca delle informazioni.
- **A3:** π è due volte derivabile e strettamente convessa
  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.

Di conseguenza il processo decisionale della impresa può essere formalizzato in questo modo:

$$\max_{I \geq 0} \{R(I) - I\} = \{X - [\pi(I, v)]aX - I\}$$

L'impresa sceglie il livello di investimento I per massimizzare il rendimento $R(I) - I$, che è dato dal ricavo meno il costo dell'investimento.

La condizione del primo ordine per questo problema è:

$$-\frac{\partial \pi(I,v)}{\partial I} aX = 1$$

Risolvendo questa equazione si ottiene il livello ottimale di investimento I*, dove il beneficio marginale (riduzione della perdita attesa) è uguale al costo marginale.

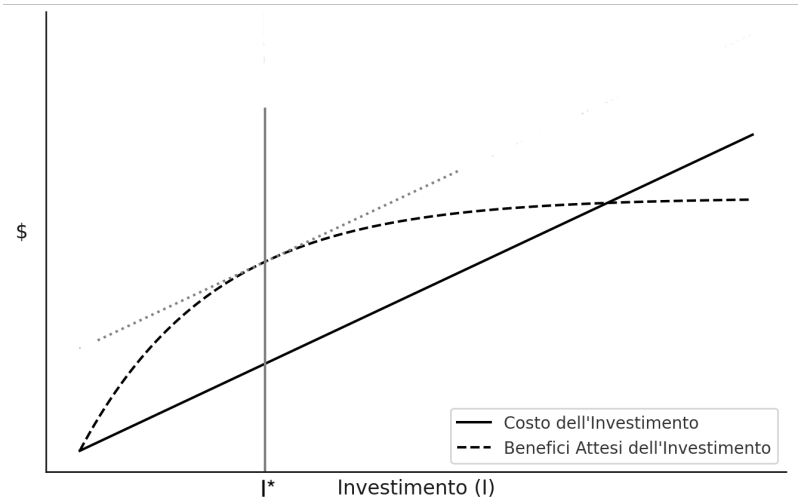

Figura 2.1: Analisi costi benefici

A questo punto gli autori per derivare una soluzione considerano due classi di funzioni di probabilità esplicite di violazione della sicurezza, che rispettano le Assunzioni A1-A3.

La prima classe di funzioni presa in esame è del tipo:

$$\pi_1(I,v) = \frac{v}{(\alpha I + 1)^{\beta}}$$

Questa funzione è scelta sia per la sua semplicità sia per la sua linearità rispetto alla vulnerabilità come mostrato in figura 2.2 dove possiamo osservare il valore atteso della perdita delle informazioni all'aumentare della vulnerabilità per diversi livelli di investimento

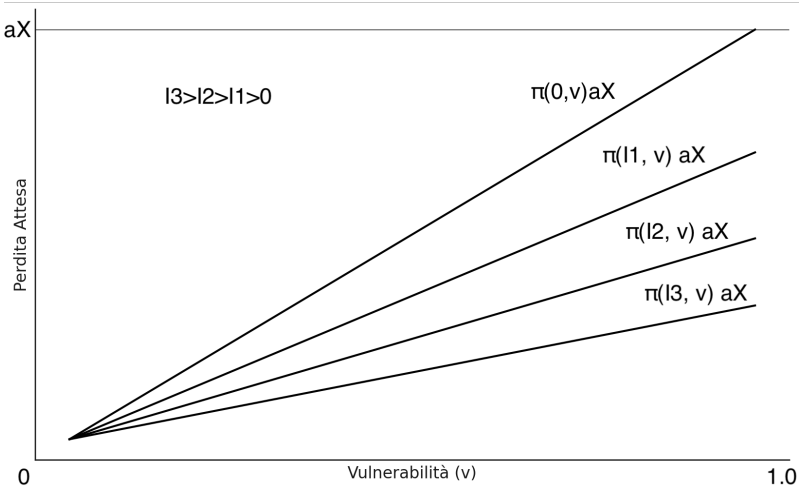

Figura 2.2: Analisi costi benefici

Da qui, come mostrato in figura 2.3, dimostrano come il livello ottimale di in vestimento sia 0 sotto una certa soglia di vulnerabilità ma aumenti all'aumentare di quest'ultima.

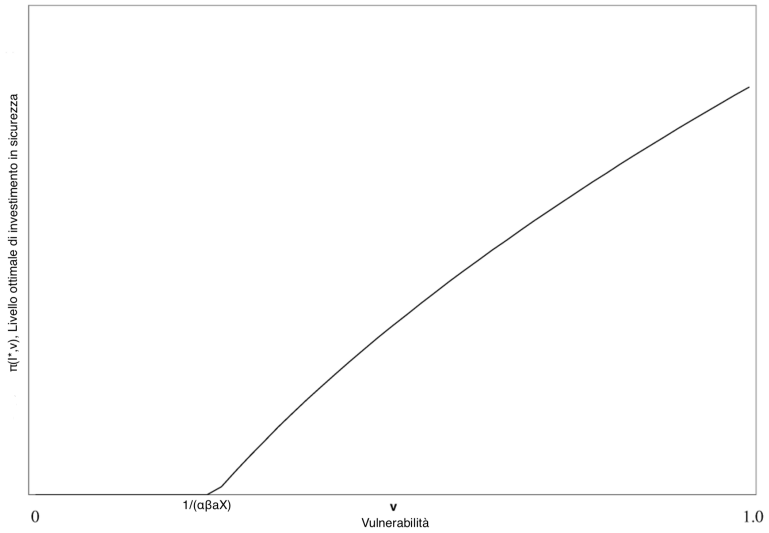

Figura 2.3: Analisi costi benefici

Nel caso della seconda classe di funzioni invece del tipo:

$$\pi_2(I, v) = v^{\alpha I+1}$$

Caratterizzata da una relazione non più lineare in v come mostrato in Figura 4, dove troviamo graficate diverse curve che rappresentano un membro diverso della classe di funzione 2 parametrizzata variando $I > 0$ per un valore fisso di a.

Questa classe di funzioni di probabilità di violazione della sicurezza ha la proprietà che il costo per proteggere set di informazioni altamente vulnerabili diventa estrema-

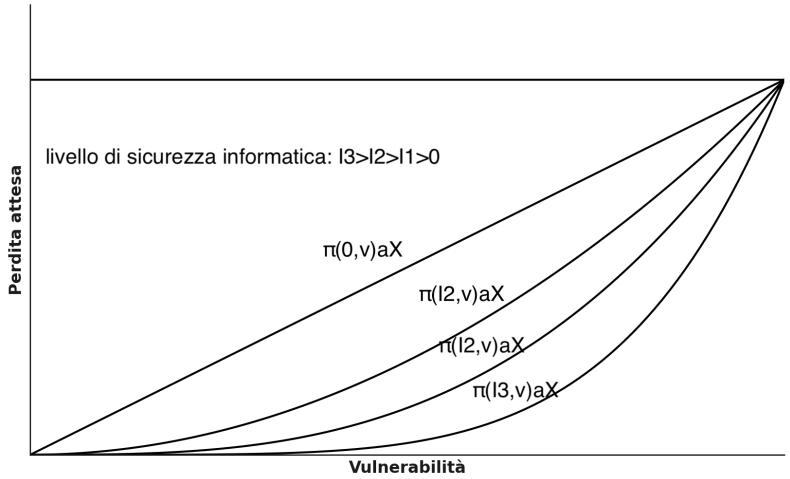

Figura 2.4: Analisi costi benefici

mente elevato man mano che la vulnerabilità del set di informazioni diventa molto grande. La conseguenza è che l'investimento ottimo di I non è più strettamente crescente in V ma assume una forma a "U" tale per cui diventa più conveniente non investire sia per livelli molto bassi che per livelli molto alti di vulnerabilità come mostrato in figura 2.5

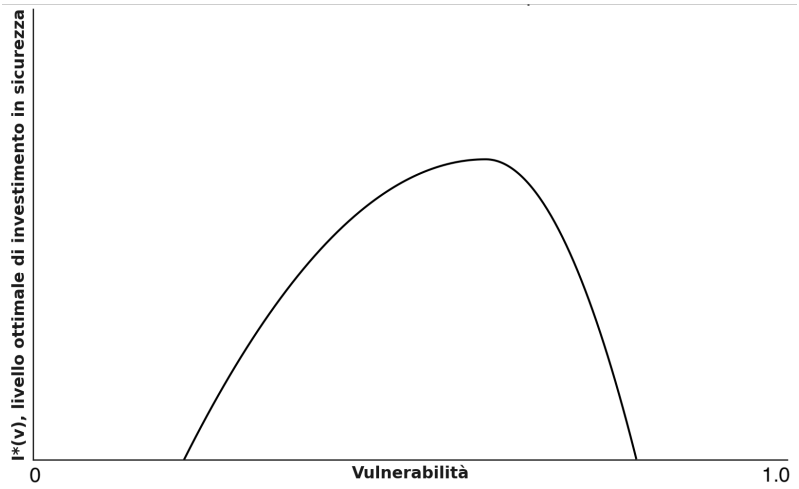

Figura 2.5: Analisi costi benefici

Attraverso queste due classi di funzioni gli autori dimostrano come le imprese dovrebbero essere particolarmente prudenti nel decidere dove allocare le risorse per la sicurezza delle informazioni in quanto come si evince dalle figure 3 e 5 data una certa perdita potenziale potrebbe essere più conveniente proteggere maggiormente le informazioni più vulnerabili (se ci si trova nel caso della funzione di classe 1) oppure potrebbe convenire concentrare i propri sforzi su informazioni con vulnerabilità medie (nel caso di funzioni di classe 2).

Oltre a questo però gli autori dimostrano anche un ultimo fatto, essi sottolineano

come per entrambe le ampie classi di funzioni si possa ricavare che il massimo investimento ottimo non supra mai il 36,8% (1/e) del valore della perdita attesa nel casa in cui non si effettuasse nessun investimento in sicurezza.

L'importanza pratica della di questa implicazione come guida per il processo decisionale risiede nel fatto che la cifra del 36,8% rappresenta un massimo. Per una vasta gamma di funzioni di probabilità di violazione della sicurezza appartenenti alle classi I e II, l'importo ottimale da investire nella sicurezza delle informazioni è infatti notevolmente inferiore.

Tuttavia, questo risultato ha suscitato un dibattito riguardante la sua robustezza, dando vita a nuovi filoni di letteratura che esplorano e approfondiscono le assunzioni che hanno portato a queste conclusioni.

2.3.2 Altri paper

Dopo la pubblicazione del modello di Gordon e Loeb nel 2002, che concludeva che l'investimento ottimale in sicurezza informatica fosse limitato superiormente al 36,8% del valore della perdita attesa senza protezione, questo risultato è stato oggetto di discussione tra i ricercatori. Tale dibattito ha portato a indagare ulteriormente la natura di questo limite superiore, concentrandosi in particolare sulle assunzioni riguardanti la funzione di rendimento degli investimenti. Questo ha dato vita a un gruppo di ricerche che hanno proposto diverse nuove classi di queste funzioni.

Hausken (2006) nel suo studio rilassa l'assunzione A3, ossia dei rendimenti marginali decrescenti, indagando l'effetto di diverse ipotesi di rendimento della funzione di probabilità post investimento. Egli osserva quattro diversi tipi di rendimento:

- Decrescente;
- Prima decrescente e poi crescente (funzione logistica);
- Crescente;
- Costante.

dimostrando come il limite del 36,8% sia effettivamente superabile modificando questa condizione.

In particolare, per quanto riguarda la funzione logistica, questa viene analizzata in quanto il suo andamento generale spiega una ampia gamma di fenomeni, dalla crescita della popolazione al contagio dei virus, e potrebbe risultare appropriata anche per gli investimenti in sicurezza. Secondo questa funzione, gli investimenti iniziali in misure di sicurezza avrebbero un impatto modesto poiché gli hacker potrebbero essere in grado di aggirare facilmente difese non all'avanguardia. Solo con l'introduzione di misure più sostanziali e a fronte di investimenti maggiori, la vulnerabilità comincia a diminuire rapidamente, fino ad assestarsi su un plateau dove l'azienda ha ormai installato i migliori strumenti disponibili e quindi non può più migliorare.

Con queste premesse, Hausken dimostra che l'investimento ottimale in sicurezza per la funzione logistica quando la vulnerabilità è bassa, è nullo, poiché i benefici derivanti dalla riduzione della vulnerabilità non giustificano i costi sostenuti. Tuttavia, per vulnerabilità intermedie, l'investimento ottimale aumenta significativamente: l'impatto delle misure di sicurezza diventa rilevante, riducendo rapidamente la probabilità di una violazione. Per vulnerabilità alte, l'investimento continua a crescere in modo concavo. Questo riflette i rendimenti marginali decrescenti, dove ogni ulteriore incremento nell'investimento produce benefici sempre minori. In questa fase, l'investimento ottimale può superare il 36,8% della perdita attesa ante investimento, contrariamente a quanto avviene con funzioni di rendimenti marginali puramente decrescenti. In generale, sebbene le soglie specifiche possano variare in base ai parametri della funzione, il modello suggerisce che le aziende dovrebbero concentrare gli investimenti in sicurezza quando la vulnerabilità delle informazioni è

intermedia, poiché è in questo range che l'investimento ha un impatto significativo e giustificabile.

Per quanto riguarda le funzioni con rendimenti crescenti e lineari, entrambe condividono un comportamento simile in termini di investimento ottimale. Nella funzione di rendimento crescente, ogni unità aggiuntiva di investimento in sicurezza porta a benefici sempre maggiori. Questo tipo di funzione implica che le aziende sono incentivate a investire continuamente, poiché i rendimenti marginali aumentano con l'investimento. Il comportamento di investimento è descritto come "bang-bang", dove l'investimento è zero per basse vulnerabilità, ma salta a un livello elevato per vulnerabilità intermedie e alte.

Analogamente, nella funzione lineare, i benefici marginali degli investimenti in sicurezza sono costanti, il che significa che ogni unità di investimento produce sempre lo stesso livello di beneficio. Le aziende investono costantemente fino a quando il costo marginale dell'investimento non supera il beneficio marginale ottenuto. Anche in questo caso, il comportamento di investimento può essere di tipo "bang-bang", in cui l'investimento è zero per basse vulnerabilità e massimo per vulnerabilità intermedie e alte.

Per entrambe le funzioni, l'investimento ottimale può superare il limite del 36,8% della perdita attesa ante investimento. Nella funzione crescente, l'investimento aumenta continuamente con l'aumento della vulnerabilità, mentre nella funzione lineare, l'investimento è proporzionale alla vulnerabilità iniziale e alla perdita attesa. Willemson (2006), che considera funzioni di probabilità lineari per indagare ulteriormente il caso di rendimenti marginali costanti, dimostra che, poiché questa specificazione implica che gli attacchi informatici possono essere completamente neutralizzati investendo a sufficienza nella sicurezza, il limite superiore sull'investimento può arrivare al 100%. Le prescrizioni per entrambe le funzioni suggeriscono una maggiore enfasi sugli investimenti aggressivi in presenza di alta vulnerabilità e investimenti uniformi e continui senza picchi significativi per la funzione lineare.

Un secondo gruppo di articoli decide invece di indagare le condizioni generiche che le funzioni di probabilità devono soddisfare per avere certe caratteristiche, anziché concentrarsi su funzioni di probabilità di violazione della sicurezza esplicite.

Baryshnikov (2012) e Lelarge (2012) generalizzano lo studio di Gordon e Loeb (2002) derivando una proprietà matematica che le funzioni di probabilità devono soddisfare affinché l'investimento ottimale sia limitato superiormente. Essi dimostrano che, se una funzione di probabilità è non crescente e ha una convessità logaritmica in relazione all'investimento (I), allora l'investimento ottimale è limitato al 36,8% (circa $1/e$) della perdita attesa senza protezione.

La convessità logaritmica implica sempre la proprietà A3, mentre A3 non implica sempre la convessità logaritmica. Questo spiega perché gli articoli discussi nel paragrafo precedente trovano limiti superiori oltre il 36,8%; la maggior parte delle funzioni di probabilità esplicite considerate non soddisfano la proprietà A3 e, di conseguenza, non soddisfano nemmeno la più restrittiva proprietà di convessità logaritmica

Willemson (2010) osserva che una funzione generica di probabilità di violazione della sicurezza dovrebbe soddisfare la ragionevole proprietà di essere strettamente crescente in relazione alla variabile v e per questo motivo, suggerisce di estendere questo insieme di assunzioni e includere che la funzione sia positiva per qualsiasi livello di investimento (I).

In aggiunta a questi studi, altri lavori hanno cercato di estendere ulteriormente il modello base di Gordon e Loeb, aggiungendo aspetti che mirano a riflettere in modo più accurato la realtà.

Gordon et al. (2003a) e Krutilla et al. (2021) introducono la dimensione temporale nelle decisioni di investimento in cybersecurity. In particolare, Gordon et al. (2003a) analizzano il problema dell'investimento attraverso la teoria delle opzioni reali. A differenza degli studi precedenti, in questo modello l'azienda non si trova a decidere solo se investire immediatamente, ma anche quando farlo. Questa considerazione è cruciale e realistica poiché gli investimenti in sicurezza informatica sono generalmente irreversibili: una volta effettuati, è tecnicamente difficile o costoso disinvestire e recuperare le risorse, e l'incertezza sulle violazioni della sicurezza permane. L'irreversibilità combinata con l'incertezza può rendere vantaggioso posticipare l'investimento. Ad esempio, in settori dove gli attacchi informatici sono rari (alta incertezza), la decisione di rimandare un investimento irreversibile può risultare più preziosa rispetto a settori dove gli attacchi sono frequenti (bassa incertezza). Gordon et al. (2003a) evidenziano che per un'azienda è conveniente investire immediatamente solo se il valore attuale netto dell'investimento è non solo positivo, ma anche superiore al valore dell'opzione di posticipare l'investimento fino a quando l'incertezza diminuisce, come in caso di una violazione della sicurezza.

Krutilla et al. (2021) invece ampliano il modello di Gordon e Loeb (2002) considerando le decisioni di investimento di un'azienda su un orizzonte temporale infinito, dove gli asset di cybersecurity (software, hardware e capitale umano utilizzato come sistema di sicurezza) sono soggetti a deprezzamento e i benefici netti dell'investimento vengono scontati. Gli autori dimostrano che l'investimento ottimale in cybersecurity è negativamente influenzato dalla somma del tasso di deprezzamento e del tasso di sconto. Poiché le evidenze empiriche suggeriscono che questa somma è solitamente inferiore a uno, mentre per definizione è pari a uno nel modello statico di Gordon e Loeb (2002), Krutilla et al. (2021) concludono che un'analisi su un singolo periodo potrebbe sottostimare la dimensione ottimale dell'investimento.

Un ultimo aspetto importante indagato, che mira a completare il modello di Gordon e Loeb, riguarda l'avversione al rischio delle aziende.

Mentre i lavori discussi finora presuppongono aziende neutrali al rischio, Huang et al. (2008) considerano il problema dell'investimento per un'azienda avversa al rischio e trovano due risultati interessanti che estendono Gordon e Loeb (2002).

- **Primo:** quando l'azienda affronta una minaccia descritta dalla funzione di probabilità, il livello ottimale di investimento in sicurezza non è più limitato al 36,8% della perdita attesa senza protezione.

- **Secondo:** l'investimento ottimale non aumenta necessariamente con l'avversione al rischio.

Oltre alle violazioni informatiche, un'azienda avversa al rischio considererebbe infatti anche il rischio dell'investimento stesso (ad esempio, le contromisure potrebbero non funzionare come previsto); la decisione di investimento è quindi influenzata dal bilanciamento tra i due tipi di rischio: man mano che l'investimento in sicurezza aumenta, il rischio dell'investimento potrebbe superare il rischio della sicurezza.

2.4 Interdipendenze Tecniche

La letteratura sugli investimenti in cybersicurezza che considera le interdipendenze tecniche rappresenta un'evoluzione significativa rispetto agli studi iniziali che trattavano le imprese come entità indipendenti. Questo filone di ricerca esamina come le decisioni di investimento in cybersicurezza di una singola impresa possano influenzare e essere influenzate dalle decisioni di altre imprese che operano all'interno dello stesso network informatico.

In un contesto di interdipendenze tecniche, le imprese non operano in isolamento; piuttosto, sono connesse attraverso una rete comune di sistemi informatici. Questo implica che l'investimento in cybersicurezza di un'impresa può avere effetti positivi non solo per sé stessa ma anche per tutte le altre imprese collegate alla stessa rete. Tali effetti sono comunemente noti come "spillover" tecnici. Quando un'impresa investe in misure di sicurezza, riduce la probabilità di attacchi informatici che possono colpire l'intera rete, migliorando così la sicurezza complessiva del network.

Il meccanismo fondamentale alla base delle interdipendenze tecniche si basa sulla condivisione dei benefici derivanti dagli investimenti in sicurezza. In una rete comune, l'aumento delle difese informatiche di un'impresa diminuisce la vulnerabilità dell'intera rete, offrendo un livello di protezione che si estende oltre i confini dell'impresa stessa. Questo comporta un dilemma strategico: mentre ogni impresa può beneficiare degli investimenti altrui, potrebbe essere tentata di ridurre il proprio investimento confidando nella protezione fornita dalle altre. Questo fenomeno, noto come "free riding," può portare a livelli subottimali di investimento in sicurezza se non adeguatamente gestito.

Per esemplificare questa branca di letteratura, il modello di Fedele e Roner è una buona base per comprendere e comparare i risultati con i modelli precedenti e quelli futuri.

2.4.1 Il modello

Il modello di Fedele e Roner rappresenta un quadro teorico avanzato per studiare gli investimenti in cybersicurezza in presenza di interdipendenze tecniche. Questo modello considera un insieme di imprese connesse attraverso una rete comune di sistemi informatici, analizzando come i benefici degli investimenti in sicurezza si estendano alle altre imprese della rete. Le interazioni tra le imprese sono quindi cruciali per comprendere il comportamento di investimento ottimale in questo contesto. Le imprese sono caratterizzate da neutralità al rischio e devono decidere quanto investire per proteggere un set di informazioni, tenendo conto delle interdipendenze tecniche.

Denotiamo con:

- X: Il valore delle informazioni dell'impresa, definito come i suoi ricavi.
- $t \in [0, 1]$: La probabilità di subire un attacco informatico, che per semplicità consideriamo uguale a 1.
- $v \in [0, 1]$: La probabilità di successo dell'attacco prima che l'investimento per migliorare le difese sia stato effettuato. Che consideriamo pari a 1.
- $a \cdot X, a \in [0, 1]$: La perdita monetaria dovuta all'attacco in caso si verificasse.

L'impresa deve quindi decidere il livello di investimento monetario $I \geq 0$ per ridurre la probabilità di successo dell'attacco v.

La decisione che limporesa si trova ad affrontare può essere formalizzata nel seguente modo:

$$\max : R(I) - I = \{X - [\pi(I, v)] \cdot aX - I\}$$

In presenza di interdipendenze tecniche, la probabilità post investimento di successo dell'attacco informatico è data dalla funzione $\pi(I, v) \in [0, v]$ ed è caratterizzata dalle stesse assunzioni viste per il modello di Gordon e Loeb (2002) ed ha forma :

$$\pi(I, v) = \frac{1(v = 1)}{I_i - eI_j + 1}$$

In questo modo viene modellizzato che l'investimento di un'impresa riduce non solo la probabilità di una violazione per sé stessa ma anche per tutte le altre imprese collegate alla rete. Questa tipologia di funzione di probabilità è particolarmente utile per effettuare un confronto con il caso precedente di assenza di interdipendenze, poiché l'unico fattore che distingue e separa questa funzione da una che non considera interdipendenze è il parametro e. Se e è maggiore di 0, implica l'esistenza di interdipendenze tecniche; se e è uguale a 0, non vi sono interdipendenze.

A questo punto l'impresa i sceglie il livello di investimento I_i per massimizzare il suo rendimento $R_T(I_i, I_j) - I_i$, che è dato dal ricavo meno il costo dell'investimento e la perdita attesa ridotta dall'investimento proprio e degli altri.

La condizione del primo ordine per questo problema è:

$$-\frac{d(\pi I, v)}{dI} = 1$$

Risolvendo questa equazione si ottiene il livello ottimale di investimento I_i^*, dove il beneficio marginale dell'investimento (riduzione della perdita attesa) è uguale al costo marginale. La soluzione ottimale riflette l'equilibrio tra i benefici condivisi dell'investimento in sicurezza in una rete interconnessa e i comportamenti di free riding che possono emergere

La soluzione è:

$$I_T^* = \frac{\sqrt{aX} - 1}{1 + e}$$

che, comparata alla soluzione senza interdipendenze, risulta essere sempre minore per $e > 0$. Da questo si deduce che lo spillover tecnico induce il free-riding e che, quanto più grande è lo spillover, tanto maggiore è il free-riding.

$$I_T^* = \frac{\sqrt{aX} - 1}{1 + e} < I^* = \frac{\sqrt{aX} - 1}{1}$$

Rilassando l'ipotesi che il numero di aziende sia limitato a 2 e espandendo il modello a N generico > 2, il processo decisionale della singola impresa non cambia. Infatti, la funzione obiettivo da massimizzare rimane:

$$\max : R(I) - I = \{X - [\pi(I, v)] \cdot aX - I\}$$

La presenza di più aziende nella decisione compare nella funzione di probabilità nella seguente forma:

$$\pi(I, v) = \frac{1}{I_i + e \cdot \sum_{j \neq i} I_j + 1} \quad \text{con} \quad v = 1$$

Come nel caso precedente, il parametro e regola la presenza degli spillover o la sua assenza, mentre la sommatoria esprime la somma degli effetti congiunti di spillover degli altri investimenti sul network.

La soluzione in questo caso diventa:

$$I_T^* = \frac{\sqrt{aX} - 1}{1 + (N - 1) \cdot e}$$

Da questa soluzione si deduce nuovamente come il numero di imprese, all'aumentare, aumenti il free-riding. Di conseguenza, N impatta negativamente aumentando l'underinvestment e il relativo fallimento di mercato.

2.4.2 Investimento socialmente efficiente

L'investimento socialmente efficiente in cybersicurezza si riferisce al livello di investimento ottimale che massimizza il benessere complessivo della società, piuttosto che il rendimento individuale di ciascuna impresa. In altre parole, si tratta del livello di investimento che, tenendo conto delle interdipendenze tra le imprese, minimizza i costi totali derivanti dai cyberattacchi per l'intera rete di imprese.

Nel contesto delle interdipendenze tecniche, l'investimento socialmente efficiente considera non solo i benefici diretti per l'impresa che effettua l'investimento, ma anche gli spillover positivi che migliorano la sicurezza delle altre imprese connesse alla stessa rete informatica. Questo approccio contrasta con quello delle singole imprese che, mirando a massimizzare i propri profitti, potrebbero investire meno del necessario in sicurezza, confidando nei benefici degli investimenti altrui.

Il modello di Fedele e Roner permette di confrontare l'investimento individuale con quello socialmente efficiente, mettendo in evidenza le differenze tra il comportamento ottimale per un singolo attore e quello ottimale per la collettività. Attraverso l'analisi del livello di investimento che massimizza il benessere complessivo, è possibile identificare la misura in cui il free-riding riduce l'investimento in sicurezza e suggerire interventi di policy per correggere questo fallimento di mercato.

In questa sezione, verrà esamianto come il modello di Fedele e Roner determini l'investimento socialmente efficiente, analizzando le condizioni che portano a un livello ottimale di sicurezza per l'intera rete di imprese e confrontando questo risultato con gli investimenti determinati dalle singole imprese. Questo confronto ci permetterà quindi di capire meglio le dinamiche del free-riding e le possibili soluzioni per incentivare investimenti adeguati in cybersicurezza.

Il calcolo del livello di investimento socialmente efficiente avviene tramite la funzione:

$$I_T^{E*}(N) = \max N \times [R_T(I) - I] = N \times \{X - [\pi(I, v)] \cdot aX - I\}$$

che, anziché massimizzare il beneficio della singola impresa, mira a massimizzare il benessere collettivo. In questo contesto, l'obiettivo è trovare il livello di investimento che minimizzi i costi totali derivanti dai cyberattacchi per tutte le imprese della rete, tenendo conto degli spillover tecnici positivi.

La funzione di probabilità, in presenza di interdipendenze tecniche, diventa:

$$\pi(I, v) = \frac{1}{I + e \cdot (N - 1) \cdot I + 1}$$

che riflette il fatto che l'investimento di un'impresa riduce la probabilità di una violazione non solo per sé stessa, ma anche per tutte le altre imprese connesse alla rete.

La soluzione a questo punto diventa:

$$I_T^E(N) = \frac{\sqrt{[1 + (N-1)e]aX - 1}}{1 + (N-1)e}$$

Confrontando questo risultato con quello trovato precedentemente per l'investimento individuale ottimale, si evince che:

$$I_T^{E*} > I_T^* \quad \text{sempre per} \quad N \geq 2 \quad \text{e} \quad e > 0$$

Dal confronto tra queste due soluzioni si deduce che l'investimento socialmente efficiente è generalmente maggiore dell'investimento individuale ottimale. Questo è dovuto al fatto che le singole imprese, agendo in modo indipendente, tendono a sottovalutare gli spillover positivi che i loro investimenti in cybersicurezza generano per l'intera rete. Di conseguenza, il livello di investimento risultante dalle decisioni individuali è inferiore a quello che sarebbe ottimale dal punto di vista collettivo.

Questa discrepanza evidenzia il problema del free-riding: le imprese beneficiano degli investimenti in sicurezza altrui senza contribuire proporzionalmente, portando a un underinvestment in cybersicurezza. Aumentare il numero di imprese connesse alla rete amplifica ulteriormente questo problema, aumentando il grado di free-riding e portando a livelli ancora più bassi di investimento complessivo rispetto a quello socialmente efficiente.

Pertanto, per correggere questo fallimento di mercato, potrebbero essere necessari interventi di policy che incentivino comportamenti cooperativi tra le imprese e promuovano investimenti adeguati in cybersicurezza, garantendo una maggiore sicurezza collettiva.

2.4.3 Altri paper

Oltre al modello di Fedele e Ronner, che fornisce un quadro completo delle dinamiche di interdipendenza tra imprese attraverso gli spillover tecnici, è utile considerare altri contributi significativi nella letteratura che estendono e arricchiscono questo modello. Questi contributi mirano a rilassare alcune assunzioni del modello principale e ad esplorare aspetti più realistici che aggiungono nuove prospettive sulle sfide e sulle dinamiche degli investimenti in sicurezza informatica.

Varian (2004) esamina un contesto in cui gli spillover tecnici tra le imprese sono massimi (e=1 nel modello di Fedele Ronner). In questo scenario, ogni investimento in sicurezza fatto da un'impresa ha il massimo effetto positivo possibile sulle altre imprese collegate nella rete. Varian conclude che, nonostante l'aumento degli spillover tecnici, gli investimenti in sicurezza informatica rimangono subottimali. Questo accade perché le imprese tendono a sfruttare gli investimenti delle altre per ridurre i propri costi. Anche con spillover massimi, l'incentivo a investire rimane insufficiente, evidenziando la necessità di interventi esterni o politiche che incentivino adeguatamente gli investimenti in sicurezza.

Böhme (2012) introduce una distinzione cruciale tra il rischio diretto di attacchi informatici e il rischio indiretto di contagio da altre imprese all'interno della rete. Questo approccio riconosce che le imprese devono preoccuparsi non solo degli attacchi diretti, ma anche del rischio di contagio proveniente da altre imprese collegate. L'analisi di Böhme rivela che che la presenza di rischio indiretto complica ulteriormente la decisione di investimento, poiché le imprese devono bilanciare la protezione contro attacchi diretti e il rischio di contagio portando ad un ulteriore accentramento dell'underinvestment.

Grossklags et al. (2008) arricchiscono ulteriormente la discussione differenziando tra due tipi di investimenti in sicurezza : autoprotezione e autoassicurazione. L'autoprotezione riduce la probabilità che si verifichi una violazione della sicurezza, mentre l'autoassicurazione limita l'entità del danno in caso di attacco. Gli autori trovano che gli investimenti di autoprotezione possono essere subottimali dal punto di vista del welfare a causa degli spillover tecnici, che creano incentivi al free-riding. D'altro canto, gli investimenti di autoassicurazione sono sempre a livello socialmente efficiente poiché non producono esternalità. Questa distinzione sottolinea l'importanza di comprendere i diversi tipi di investimenti in sicurezza e il loro impatto sulla rete complessiva.

A questo riguardo Tim J. Boonen in un recente studio del 2023 esamina come le aziende possano mitigare il rischio informatico attraverso investimenti in sicurezza informatica e l'acquisto di assicurazioni informatiche, utilizzando un modello di rete per analizzare le interazioni tra aziende interconnesse. Gli autori trovano che l'investimento in sicurezza e l'acquisto di assicurazioni sono complementari strategici, il che significa che un aumento nella copertura assicurativa porta a una diminuzione degli investimenti in sicurezza e viceversa. Lo studio stabilisce l'esistenza e l'unicità di un equilibrio di Nash per queste decisioni e fornisce esempi numerici per diverse strutture di rete.

Acemoglu et al. (2016) aggiungono una nuova dimensione all'analisi introducendo il concetto di attaccanti strategici nel contesto della sicurezza della rete. Gli attaccanti strategici scelgono di mirare alle parti più vulnerabili della rete per massimizzare il danno complessivo. Questo induce le aziende a comportarsi in modo strategico, aumentando i loro investimenti in sicurezza per evitare di essere bersagliate. Gli autori evidenziano che tali attacchi creano sia esternalità positive che negative. Le esternalità positive derivano dal fatto che un maggiore investimento in sicurezza riduce la probabilità di infezione per il resto della rete. Tuttavia, le esternalità negative emergono perché un elevato investimento in sicurezza in un'azienda aumenta la probabilità che l'attaccante scelga un'altra azienda come bersaglio. Una delle principali conclusioni di Acemoglu et al. è che in presenza di attacchi strategici, le aziende tendono a sovrainvestire in sicurezza rispetto al livello socialmente ottimale. Questo accade perché, oltre a proteggersi, le aziende cercano di scoraggiare gli attacchi. Tale comportamento induce un "effetto di corsa agli armamenti" dove ogni azienda continua ad aumentare i propri investimenti per dissuadere l'attaccante, amplificando le esternalità negative per le altre aziende. Questo sovrainvestimento è una conseguenza delle complementarità strategiche nelle decisioni di investimento, dove il livello di investimento desiderato da un nodo aumenta in risposta agli investimenti degli altri nodi, poiché tali investimenti aumentano la probabilità che l'attaccante prenda di mira il nodo in questione.

2.5 Interdipendenze di Mercato

La letteratura sugli investimenti in cybersicurezza che considera le interdipendenze di mercato rappresenta un'ulteriore evoluzione significativa rispetto agli studi iniziali che trattavano le imprese come entità indipendenti. Questo filone di ricerca esamina come le decisioni di investimento in cybersicurezza di una singola impresa possano influenzare e essere influenzate dalle decisioni di altre imprese che operano nel medesimo mercato competitivo.

In un contesto di interdipendenze di mercato, le imprese non operano in isolamento. Piuttosto, competono direttamente nel mercato dei prodotti. Questo implica che l'investimento in cybersicurezza di un'impresa può avere effetti positivi o negativi non solo per sé stessa ma anche per i suoi concorrenti. Tali effetti sono comunemente noti come "spillover" di mercato. Quando un'impresa investe in misure di sicurezza riduce la probabilità di subire attacchi informatici che potrebbero compromettere la sua operatività, migliorando così la sua posizione competitiva nel mercato.

Il meccanismo fondamentale alla base delle interdipendenze di mercato si basa sul trasferimento di clientela e quote di mercato in seguito a un attacco informatico. Se un'impresa subisce un attacco e vede compromessa la propria capacità operativa, i suoi clienti potrebbero rivolgersi ai concorrenti che non sono stati colpiti. Questo comporta un dilemma strategico: mentre ogni impresa può beneficiare delle debolezze dei concorrenti, potrebbe essere tentata di ridurre il proprio investimento confidando sulla possibilità di attrarre clienti dai concorrenti compromessi. Questo fenomeno può portare a livelli di investimento in sicurezza che sono eccessivi rispetto a quanto socialmente ottimale.

Nel contesto delle interdipendenze di mercato, il modello di Fedele e Roner rappresenta una buona base per comprendere e comparare i risultati con i modelli precedenti e quelli futuri. Essi analizzano come gli investimenti in cybersicurezza possano essere influenzati dalle dinamiche competitive e dagli spillover di mercato, evidenziando la tendenza delle imprese a investire eccessivamente in sicurezza per proteggere la propria posizione nel mercato. Questo comportamento può essere dannoso per l'efficienza complessiva del mercato, suggerendo la necessità di politiche che incentivino una cooperazione più equilibrata tra le imprese.

2.5.1 Il modello

Il modello di Fedele e Roner rappresenta un quadro teorico avanzato per analizzare queste dinamiche. Nel loro modello, considerano $N \geq 2$ imprese simmetriche e neutrali al rischio che affrontano la stessa probabilità di subire un attacco informatico ($t = 1$) e competono direttamente sul mercato dei prodotti, ma operano con sistemi informatici non interconnessi. Questo implica che l'investimento in cybersicurezza di ciascuna impresa per ridurre la propria probabilità di violazione non influisce sul livello di protezione goduto dai concorrenti, escludendo quindi gli spillover tecnici.

Il modello si sviluppa in due fasi principali:

1. Il parametro X denota il ricavo di mercato totale, che è condiviso equamente tra le imprese concorrenti. Pertanto, la quota di ricavo che spetta a ciascuna impresa è $\frac{X}{N}$.
2. Si assume che le imprese che subiscono un attacco informatico perdano le loro quote di ricavo, che vengono acquisite dai concorrenti non colpiti. Con una semplificazione, il parametro a è impostato uguale a 1, indicando che l'intero ricavo è perso in caso di attacco.

In caso di duopolio, la decisione che l'impresa singola si trova ad affrontare è rappresentata dalla seguente funzione:

$$\max_{I_i \geq 0} R_M(I_i, I_j) - I_i = \left[\frac{X}{2} + \frac{1}{I_i + 1} \left(-\frac{X}{2} \right) + \left(1 - \frac{1}{I_i + 1} \right) \frac{1}{I_j + 1} \frac{X}{2} - I_i \right]$$

Questa equazione descrive il rendimento atteso $R_M(I_i, I_j)$ meno il costo dell'investimento I_i per l'impresa i, tenendo conto degli investimenti I_i e I_j delle due imprese nel duopolio.

L'equazione mostra come il rendimento di un'impresa dipenda non solo dal proprio investimento in sicurezza, ma anche dall'investimento del concorrente. La prima parte dell'equazione $\frac{X}{2}$ rappresenta la quota di mercato iniziale. La seconda parte, $\frac{1}{I_i+1} \left(-\frac{X}{2}\right)$, mostra la perdita di ricavi in caso di attacco subito dall'impresa i. La terza parte, $\left(1 - \frac{1}{I_i+1}\right) \frac{1}{I_j+1} \frac{X}{2}$, rappresenta il guadagno di ricavi derivante dalla perdita del concorrente j in caso di attacco subito da quest'ultimo. Infine, l'ultimo termine $-I_i$ è il costo dell'investimento in sicurezza per l'impresa i.

Risolvendo il problema per trovare un equilibrio di Nash simmetrico, si trova che il livello ottimale di investimento è dato dall'espressione:

$$I_M^*(2) = \frac{X + 6H^2}{6H} - 1$$

con H:

$$H = \sqrt[3]{\frac{X^2(27 - 2X)}{432} + \frac{X}{4}}.$$

Partendo da questo risultato gli autori dimostrano come $I_M^*(2)$ sia inferiore a I^* per qualsiasi valore di $X > 1$, il che significa che l'investimento in equilibrio si riduce passando dal monopolio al duopolio.

$$I_M^*(2) = \frac{X + 6H^2}{6H} - 1 < I^* = \frac{\sqrt{aX} - 1}{1}$$

Gli spillover di mercato producono quindi lo stesso risultato degli spillover tecnici. Tuttavia, operano attraverso un meccanismo diverso, che non è innescato dal free riding e può essere descritto come segue.

Una impresa monopolistica ($N = 1$) che decide di aumentare l'investimento in cybersicurezza ha maggiori probabilità di non subire alcuna violazione della sicurezza, nel qual caso ottiene l'intero ricavo di mercato X. In questo caso, l'investimento ottimale I^* sarebbe il risultato senza l'interdipendenza.

Al contrario, lo stesso investimento aggiuntivo effettuato da ciascuna impresa duopolistica $i = 1, 2$ è meno efficace perché l'impresa i ottiene l'intero ricavo di mercato X solo se il concorrente j viene colpito da un attacco informatico, la cui probabilità è inferiore a 1 per qualsiasi $I_j > 0$.

Il meccanismo degli spillover di mercato influenza quindi gli investimenti in cybersicurezza in modo diverso rispetto agli spillover tecnici, riducendo l'efficacia dell'investimento aggiuntivo in un contesto di duopolio rispetto a quello monopolistico.

2.5.2 Caso $N > 2$

Consideriamo ora il caso di un mercato con $N \geq 2$ imprese simmetriche e neutrali al rischio, che affrontano la stessa probabilità di subire un attacco informatico e competono direttamente nel mercato dei prodotti. Ogni impresa deve decidere il livello ottimale di investimento in cybersicurezza, tenendo conto delle interdipendenze di mercato e della maggiore competizione.

In questo contesto il processo decisionale della impresa è formalizzato nel modo seguente:

$$\max_{I_i \geq 0} R_M(I_1, \ldots, I_N) - I_i = \left[\frac{X}{N} + \frac{1}{I_i + 1} \left(-\frac{X}{N} \right) + \left(1 - \frac{1}{I_i + 1} \right) K - I_i \right]$$

con K specificato nell'appendice

I primi due termini all'interno delle parentesi quadre sono equivalenti ai rispettivi termini nel problema precedente, con un generico $N \geq 2$ invece che 2. Il terzo termine è, invece, diverso e dato dalla probabilità che l'impresa i non subisca alcuna violazione della sicurezza, $1 - \frac{1}{I_i+1}$, moltiplicato per un'espressione, denotata da K, che descrive il valore atteso del guadagno goduto dall'impresa i quando si trova nella posizione di catturare le quote di ricavo dei concorrenti che subiscono violazioni della sicurezza.

La soluzione implicita, denotata da $I_M^*(N)$, è monotonicamente decrescente in funzione di N. L'intuizione è che gli spillover di mercato rendono l'investimento in cybersicurezza sempre meno efficace all'aumentare di N, poiché ciascuna impresa $i = 1, \ldots, N$ ottiene l'intero ricavo di mercato X solo se tutti i concorrenti sono colpiti da attacchi informatici riusciti, la cui probabilità diminuisce con l'aumentare di N. Concludiamo quindi che l'impatto negativo degli spillover di mercato sull'investimento di equilibrio per impresa, descritto sopra nel caso di duopolio, si estende in modo graduale al caso di oligopolio con $N \geq 2$ imprese.

All'aumentare del numero di imprese nel mercato ($N > 2$), si osserva che la quota di mercato che un'impresa può guadagnare investendo in cybersicurezza diminuisce ulteriormente. Questo implica che le imprese sono meno incentivate ad investire in sicurezza, poiché l'efficacia marginale del loro investimento si riduce con l'aumento del numero di concorrenti.

In altre parole, mentre nel passaggio dal monopolio al duopolio l'investimento ottimale in cybersicurezza si riduceva a causa della presenza di un concorrente, in un mercato con più di due imprese, questa tendenza si amplifica. Ogni impresa, infatti, vede diminuire la propria capacità di ottenere ricavi aggiuntivi dal mercato a seguito di un investimento in cybersicurezza, dato che la probabilità di acquisire ricavi dai concorrenti colpiti da attacchi informatici diminuisce man mano che aumenta il numero di imprese che investono in sicurezza.

2.5.3 Investimento socialmente efficiente

Analizziamo , anche in questo caso, i risultati da una prospettiva di welfare, confrontando l'investimento di equilibrio, $I(2)$, con l'investimento socialmente efficiente quando $N = 2$, definito ancora come il valore scelto da un pianificatore sociale per massimizzare la somma dei profitti delle (due) imprese. Risolviamo quindi il seguente problema:

$$\max_{I \geq 0} 2 \times [R_M(I) - I] = \left\{ 2 \left[\frac{X}{2} + \frac{1}{I+1} \left(-\frac{X}{2} \right) + \left(1 - \frac{1}{I+1} \right) \frac{1}{I+1} \frac{X}{2} - I \right] \right\}$$

Il risultato è:

$$I_M^E(2) = \sqrt[3]{X} - 1$$

Confrontando questo risultato con quello ottenuto nei casi precedenti, notiamo che nel caso del duopolio l'investimento di equilibrio $I_M^*(2)$ risulta essere superiore rispetto all'investimento socialmente efficiente $I_M^E(2)$ il quale a sua volta risulta essere inferiore al caso del monopoliio I^*, come evidenziato nel seguente grafico:

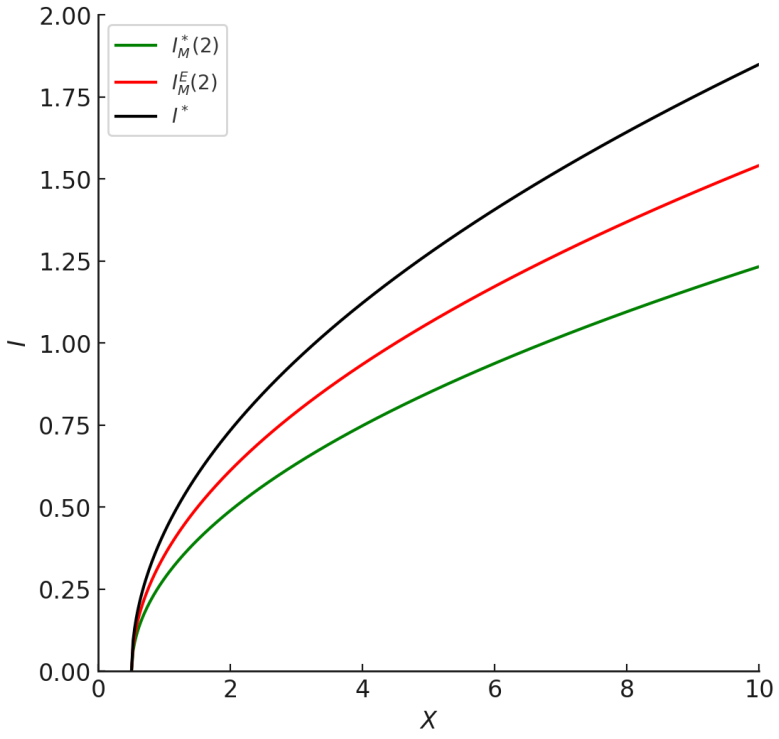

Figura 2.6: Equilibrio e livello socialmente efficiente con interdipendenze di mercato

In conclusione, l'analisi mostra che l'investimento di equilibrio delle imprese in cybersicurezza risulta superiore al livello socialmente efficiente, indicando un fenomeno di sovrainvestimento. Questo esito normativo di sovrainvestimento è dovuto a una

esternalità negativa prodotta dagli spillover di mercato. Quando un'impresa i decide di aumentare il proprio investimento I_i per ottenere una protezione migliorata, il beneficio marginale privato (ovvero l'incremento del profitto dell'impresa i) è superiore al beneficio marginale sociale (ovvero l'incremento della somma dei profitti dell'impresa i e dell'impresa j). Ciò avviene perché il primo non internalizza la ridotta possibilità per l'impresa j di guadagnare la quota di ricavi dell'impresa i.

Questo scenario evidenzia un conflitto tra l'ottimizzazione individuale delle imprese e l'efficienza collettiva del mercato. Le imprese, agendo nel proprio interesse, tendono a investire di più di quanto sarebbe socialmente ottimale, dato che ciascuna non considera l'effetto negativo che il proprio investimento ha sulla capacità dei concorrenti di trarre vantaggio dalle vulnerabilità altrui. Pertanto, emerge la necessità di politiche che possano mitigare questa esternalità negativa, come l'adozione di incentivi per una cooperazione più equilibrata tra le imprese o la regolamentazione degli investimenti in cybersicurezza. Solo attraverso tali misure si può sperare di raggiungere un livello di investimento che massimizzi il benessere sociale complessivo, equilibrando la protezione individuale delle imprese con l'efficienza collettiva del mercato.

2.5.4 Altri paper

Oltre al modello di Fedele e Ronner che abbiamo esaminato, il quale fornisce un quadro di riferimento completo delle dinamiche di interdipendenza tra imprese attraverso gli spillover tecnici, ci sono altri studi che mirano a estendere la letteratura affrontando aspetti diversi e aggiungendo nuove prospettive.

Nagurney e Nagurney introducono l'ipotesi di asimmetria informativa tra venditori e acquirenti. Questo modello si distingue dai precedenti per il fatto che i consumatori considerano il livello medio di protezione del mercato nel determinare le loro preferenze di acquisto.

Come in precedenza anche in questo modello, i venditori competono in modo non cooperativo per massimizzare i loro profitti attesi determinando le transazioni ottimali dei prodotti e gli investimenti in cybersicurezza. Gli acquirenti esprimono le loro preferenze attraverso funzioni di prezzo della domanda, che dipendono dalle richieste di prodotto e dal livello medio di sicurezza nel mercato.

Le principali conclusioni del modello di Nagurney e Nagurney indicano che, in presenza di asimmetria informativa, i venditori sono incentivati a investire in sicurezza in modo da influenzare positivamente la percezione media del livello di sicurezza del mercato. Tuttavia, gli autori mostrano che le imprese hanno un incentivo decrescente a investire in cybersicurezza man mano che aumenta il numero di concorrenti N, perché l'informazione asimmetrica impedisce sempre più ai consumatori di distinguere tra le imprese che investono adeguatamente e quelle che non lo fanno.

Confrontando questi risultati con quelli ottenuti nei casi precedenti, si nota una differenza fondamentale: mentre i modelli precedenti evidenziavano un sovrainvestimento dovuto alla competizione diretta tra imprese, il modello di Nagurney e Nagurney mostra che l'interesse dei consumatori per la sicurezza media del mercato può ridurre gli incentivi delle imprese a investire in modo eccessivo, a causa dell'impossibilità dei consumatori di valutare correttamente i livelli di investimento individuali.

Il modello di Gao e Zhong esplora invece il ruolo dei consumatori consapevoli della sicurezza utilizzando un modello di un mercato duopolistico, gli autori analizzano come le strutture di mercato e la condivisione delle informazioni influenzino gli investimenti in sicurezza informatica tra due aziende che offrono prodotti sostituibili. Un aspetto cruciale considerato dagli autori è il "demand switch ratio", ovvero la percentuale di clienti che si rivolge al concorrente in caso di violazione della sicurezza informatica di un'azienda.

Gao e Zhong osservano che un "demand switch ratio" più elevato incentiva maggiori investimenti in sicurezza da parte delle aziende, sia in un contesto di concorrenza Bertrand (dove la competizione è basata sul prezzo) che in un contesto di concorrenza Cournot (dove la competizione è basata sulla quantità). Questo perché, in un mercato dove i clienti sono più propensi a cambiare fornitore se preoccupati per la sicurezza dei loro dati, le aziende sono spinte a rafforzare i loro sistemi per non perdere clienti.

Il modello mostra che l'incentivo di ciascun duopolista a investire in sicurezza è guidato da due obiettivi principali: non solo mantenere la propria base di clienti, ma anche sottrarre clienti al concorrente. Pertanto, all'aumentare della quota di consumatori che cambiano fornitore, le imprese sono motivate a migliorare le proprie misure di sicurezza per attrarre i clienti dei concorrenti che hanno subito attacchi.

Le conclusioni principali indicano che un "demand switch ratio" più elevato risulta vantaggioso per i consumatori, spingendo le aziende a investire di più in sicurezza informatica per non perdere quote di mercato, danneggiando gli hacker, perché riduce le loro opportunità di successo.

L'articolo di Quian et al estende quello di Gao e Zhong introducendo la presenza di consumatori fedeli che non switchano a prescindere da attacchi informatici.

In un mercato con clienti fedeli, le aziende hanno una base di consumatori garantita che acquisterà i loro prodotti indipendentemente dal livello di sicurezza informatica offerto. Al contrario, i clienti "volubili", suddivisi in "aggressivi" e "non aggressivi", basano le proprie decisioni di acquisto sul livello di sicurezza informatica offerto dalle diverse aziende. I clienti volubili aggressivi sceglieranno sempre l'azienda con il livello di sicurezza più elevato, mentre i clienti non aggressivi potrebbero optare per aziende con un livello di sicurezza inferiore se influenzati da altri fattori.

Questa differenza nel comportamento dei consumatori ha un impatto diretto sulle decisioni di investimento delle aziende. In presenza di una maggioranza di clienti fedeli, le aziende saranno meno incentivate ad investire in sicurezza informatica, poiché la loro base di clienti non è sensibile a questo aspetto. Al contrario, in un mercato con un'alta percentuale di clienti volubili, le aziende saranno spinte a competere tra loro offrendo livelli di sicurezza informatica più elevati per attrarre questo tipo di clientela. Questo aspetto è particolarmente vero nel caso dei clienti volubili aggressivi, che spingono le aziende ad una competizione continua per avere un livello di sicurezza informatica superiore rispetto alla concorrenza. Questa situazione porta ad un aumento degli investimenti in sicurezza informatica, anche a livelli superiori rispetto a quelli socialmente ottimali.

In sintesi, la presenza e la tipologia di consumatori in un mercato influenza direttamente le decisioni di investimento in sicurezza informatica delle aziende: una base di clienti fedeli riduce l'incentivo ad investire, mentre una forte presenza di clienti volubili, in particolare quelli "aggressivi", spinge le aziende ad aumentare i propri investimenti in sicurezza informatica.

Garcia et al. (2014) e Sen et al. (2020) estendono i contributi esistenti modellando la competizione dinamica tra due piattaforme (software) trovando che il mercato duopolistico diventa meno concentrato nel tempo quando la piattaforma dominante subisce la maggior parte degli attacchi informatici, poiché il rivale più piccolo fornisce livelli più elevati di cybersicurezza e quindi attrae più consumatori. In altre parole, il vantaggio competitivo della piattaforma più piccola è dato dalla sua capacità di garantire una maggiore sicurezza informatica rispetto alla piattaforma dominante, inducendo una redistribuzione delle quote di mercato a suo favore.

Sen et al. (2020) trovano un beneficio non intenzionale dalla presenza di attacchi informatici: ciascuna piattaforma è maggiormente incentivata a investire in sicurezza informatica, il che aumenta la probabilità che entrambe rimangano competitive nel lungo periodo. Questo studio sottolinea che la competizione dinamica e la presenza di minacce informatiche possono avere effetti positivi sugli investimenti in sicurezza delle piattaforme, promuovendo una maggiore stabilità del mercato.

I paper finora esaminati considerano imprese che competono nello stesso mercato offrendo prodotti sostituibili. Liu et al. (2018) adottano una prospettiva diversa, analizzando due imprese che vendono prodotti complementari. Quando una delle imprese subisce un attacco informatico, anche l'altra impresa subisce un impatto negativo sulla domanda poiché i consumatori non possono sostituire un prodotto con l'altro. Gli autori trovano che un maggiore grado di complementarità tra i prodotti aumenta l'impatto positivo di un investimento in sicurezza da parte di una impresa sui ricavi della seconda impresa, la quale, a sua volta, è incentivata a investire maggiormente.

2.5.5 Recenti analisi

Il modello di de Cornière e Taylor

Una ulteriore aggiunta recente alla letteratura è rappresentata dall'articolo "A Model of Information Security and Competition" di Alexandre de Cornière e Greg Taylor, che esamina come la concorrenza sul mercato influenzi gli investimenti in sicurezza informatica da parte delle aziende. Gli autori studiano in che modo la struttura del mercato (monopolio o duopolio) e i modelli di business (basati su prezzi o pubblicità) influenzino gli incentivi delle aziende a proteggere i loro sistemi dagli attacchi informatici.

L'articolo evidenzia come i consumatori non siano tutti uguali quando si parla di sicurezza informatica. Alcuni consumatori, definiti "esperti", sono consapevoli dei rischi e ne tengono conto nelle loro decisioni di acquisto, mentre altri, "ingenui", non lo fanno.

Nel modello di prezzo, un monopolista tende a investire il livello di sicurezza socialmente ottimale quando ci sono abbastanza consumatori esperti nel mercato. Questo perché i consumatori esperti sono disposti a pagare di più per un prodotto più sicuro, incentivando il monopolista a investire in sicurezza.

Tuttavia, quando c'è concorrenza, le aziende tendono a investire meno in sicurezza. Questo perché un livello di sicurezza elevato intensifica la concorrenza sui prezzi, portando a profitti inferiori per tutte le aziende. Le aziende, in questo caso, preferiscono un livello di sicurezza più basso per mitigare la concorrenza.

Nel modello di business basato sulla pubblicità, la situazione è diversa. Un monopolista tende a sottoinvestire in sicurezza perché non può "far pagare" ai consumatori la sicurezza aggiuntiva, come farebbe in un modello di prezzo. Tuttavia, la concorrenza tra aziende che si finanziano con la pubblicità può portare a un aumento degli investimenti in sicurezza. Questo perché le aziende competono per attirare i consumatori esperti, offrendo prodotti più sicuri.

L'articolo esplora anche l'impatto che le politiche di regolamentazione hanno sulla sicurezza informatica. Gli autori mostrano come l'uso di multe per le violazioni della sicurezza e l'istituzione di sistemi di certificazione possano influenzare gli incentivi delle aziende a investire in sicurezza. Nel modello di prezzo le multe elevate si rivelano uno strumento efficace per incentivare investimenti in sicurezza. Al contrario, nei modelli basati sulla pubblicità, la combinazione di multe e sistemi di assicurazione possono essere necessari per raggiungere il livello ottimo di sicurezza.

In sintesi, l'articolo evidenzia che la relazione tra concorrenza di mercato e sicurezza informatica è complessa e dipende da una serie di fattori, tra cui la struttura del mercato, i modelli di business e il comportamento dei consumatori. Le politiche di regolamentazione, per essere efficaci, devono tenere conto di queste complessità.

2.6 Interdipendenza di mercato e tecnica

La letteratura sugli investimenti in cybersicurezza vista fino ad adesso ha analizzato in dettaglio le interdipendenze tecniche e di mercato in modo separato. Tuttavia, un ambito di studio emergente considera la combinazione di entrambe le interdipendenze, fornendo una visione più complessa e completa del comportamento delle imprese in un ambiente di sicurezza informatica interconnesso e competitivo. Questo filone di ricerca esamina come le decisioni di investimento in cybersicurezza di un'impresa siano influenzate sia dalle connessioni tecniche con altre imprese che dalla competizione di mercato.

Le interdipendenze tecniche si manifestano quando le aziende condividono una rete informatica comune, con la conseguenza che gli investimenti in sicurezza di un'impresa possono avere effetti positivi, noti come "spillover tecnici", sulla sicurezza delle altre imprese collegate. In un contesto di interdipendenza di mercato, invece, le imprese competono direttamente nel mercato dei prodotti, e un attacco informatico a una di esse può portare a una ridistribuzione delle quote di mercato a favore dei concorrenti non colpiti, creando "spillover di mercato".

Quando entrambe le forme di interdipendenza sono presenti le dinamiche degli investimenti in cybersecurity diventano particolarmente complesse. Da un lato, gli spillover tecnici incentivano un comportamento di free-riding, dove quindi le imprese potrebbero essere tentate di ridurre i propri investimenti confidando sugli investimenti altrui per proteggere la rete comune. Dall'altro gli spillover di mercato spingono le imprese a investire maggiormente in sicurezza per evitare di perdere clientela a favore dei concorrenti in caso di un attacco.

Il modello di Fedele e Roner fornisce una base teorica robusta per comprendere queste dinamiche. Analizzando l'interazione tra spillover tecnici e di mercato, il modello mostra come le imprese siano spinte a investire strategicamente in cybersicurezza per bilanciare i benefici della protezione condivisa con la necessità di mantenere una posizione competitiva nel mercato.

2.6.1 Il modello

Il modello di Fedele e Roner rappresenta un'analisi innovativa delle dinamiche di investimento in cybersecurity, combinando interdipendenze tecniche e di mercato. Questo modello considera come le decisioni di sicurezza di un'impresa siano influenzate sia dalla condivisione di una rete informatica comune (spillover tecnici) sia dalla competizione diretta nel mercato (spillover di mercato).

Si modellano dunque due imprese simmetriche neutrali al rischio il cui processo decisionale è formalizzato combinando, da un lato, il payoff nel caso delle sole interdipendenze tecniche:

$$\max_{I_i \geq 0} R_T(I_i, I_j) - I_i = \left(X - \frac{1}{I_i + eI_j + 1} aX - I_i \right)$$

ponendo $a = 1$ per semplificazione. E, dall'altro lato, i payoff nel caso delle interdipendenze di mercato:

$$\max_{I_i \geq 0} R_M(I_i, I_j) - I_i = \left[\frac{X}{2} + \frac{1}{I_i + 1} \left(-\frac{X}{2} \right) + \left(1 - \frac{1}{I_i + 1} \right) \frac{1}{I_j + 1} \frac{X}{2} - I_i \right]$$

Risultando nella seguente funzione che l'impresa si trova a massimizzare:

$$\max_{I_i \geq 0} R_{TM}(I_i, I_j) - I_i = \left[\frac{X}{2} + \frac{1}{I_i + eI_j + 1} \left(-\frac{X}{2} \right) + \left(1 - \frac{1}{I_i + eI_j + 1} \right) \frac{1}{I_j + eI_i + 1} \frac{X}{2} - I_i \right]$$

Questa rappresentazione consente di integrare sia le interdipendenze tecniche sia quelle di mercato.

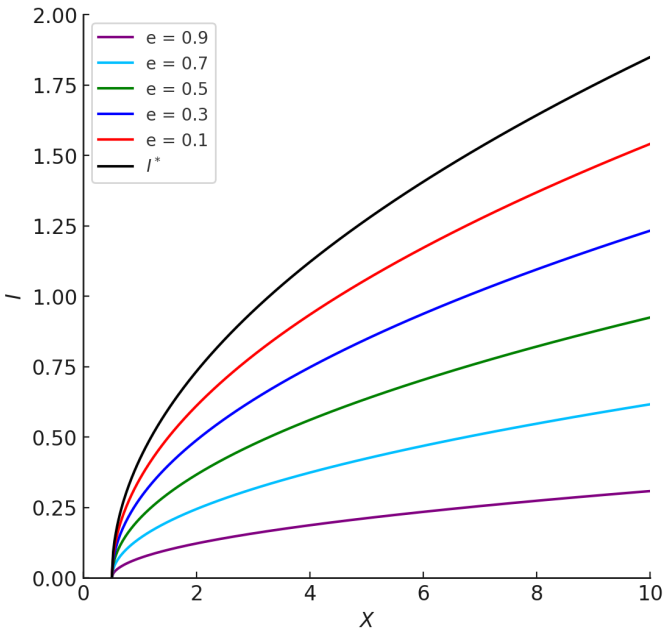

Figura 2.7: Descrizione della figura qui.

La soluzione analitica a questo problema è alquanto complessa e per questo risulta più immediato analizzare i risultati per via grafica. In figura si mostra in nero il caso del monopolio e di ottimo e a colori i casi di duopolio con diversi livelli di e che rappresenta il grado di spillover tecnico, ossia quanto l'impresa j beneficia dell'investimento in sicurezza dell'impresa i e viceversa.

Analizzando questi risultati è evidente come in ogni caso il livello di investimento sia più basso del caso del monopolio. Questo non sorprende, in quanto sia nel caso di spillover tecnici (a causa del free riding) sia nel caso di interdipendenze di mercato (a causa del fatto che per ottenere tutta la quota di mercato è necessario che il competitore venga attaccato) si verificano separatamente livelli di investimento inferiori al passaggio da monopolio a duopolio. Dunque, il risultato della combinazione dei due porta allo stesso effetto.

In aggiunta a questo fenomeno, si può osservare come all'aumentare dello spillover tecnico e quindi del livello di e, anche il livello di investimento progressivamente decresca, sempre in quanto il grado di spillover porta a un maggiore free-riding da parte delle imprese.

2.6.2 Investimento socialmente efficiente

Quando i due diversi spillover vengono considerati simultaneamente, si possono trarre interessanti spunti di riflessione dal punto di vista del benessere sociale. Gli spillover tecnici da soli determinano un sottoinvestimento, mentre gli spillover di mercato da soli portano al risultato opposto di sovrainvestimento. È quindi importante verificare in quali condizioni prevale il sottoinvestimento o il sovrainvestimento. A tal fine, l'investimento socialmente efficiente è calcolato nel modo consueto, cioè come il valore scelto da un pianificatore sociale per massimizzare la somma dei payoff delle due imprese, nel seguente modo:

$$\max_{I\geq 0} 2\times[R_{TM}(I)-I] = \left\{2\left[\frac{X}{2}+\frac{1}{I+eI+1}\left(-\frac{X}{2}\right)+\left(1-\frac{1}{I+eI+1}\right)\frac{1}{I+eI+1}\frac{X}{2}-I\right]\right\}$$

Risolvendo questo problema gli autori analizzano i doversi comportamenti del risultato di $I^*_{TM}(2)$

Il sovrainvestimento, $I^*_{TM}(2) > I^E_{TM}(2)$, tende a verificarsi per valori relativamente bassi di e. Al contrario, valori più alti di e portano al risultato opposto di sottoinvestimento, $I^*_{TM}(2) < I^E_{TM}(2)$. L'intuizione è che gli spillover di mercato prevalgono ampiamente quando e è basso. Ciò comporta che l'esternalità negativa descritta rende il beneficio sociale dell'investimento inferiore al beneficio privato e determina il sovrainvestimento. Man mano che e aumenta, l'esternalità positiva legata agli spillover tecnici diventa sempre più alta e alla fine prevale sull'esternalità negativa prodotta dagli spillover di mercato. Di conseguenza, il beneficio sociale diventa superiore al beneficio privato e si verifica il sottoinvestimento.

2.6.3 Altri papaer

Liao e Chen (2014) esaminano un numero $N \geq 2$ di aziende che possono intraprendere un investimento dicotomico in sicurezza informatica. Le aziende sono interdipendenti in modo simmetrico, il che significa che ciascuna azienda influenza in egual misura la sicurezza delle altre attraverso gli spillover tecnici. Gli autori si concentrano sul problema di un'azienda che decide di investire in sicurezza informatica e indicano con W l'aumento risultante nel suo rendimento lordo atteso. La loro analisi si chiede come W venga influenzato dal numero m di concorrenti che decidono anch'essi di investire.

Il modello presentato da Liao e Chen non determina il livello di investimento di equilibrio di Nash, ma esamina piuttosto la relazione tra l'investimento in sicurezza di una azienda singola e quello dei suoi concorrenti. L'intento è di capire se l'incentivo a investire in sicurezza aumenti o diminuisca quando più concorrenti scelgono di fare lo stesso.

L'articolo conclude che W può essere influenzato positivamente o negativamente dal numero di concorrenti che investono in sicurezza informatica. La relazione positiva si verifica quando l'investimento è particolarmente efficace, ossia quando la proporzione di aziende che non subiscono violazioni dopo l'investimento è superiore alla probabilità iniziale che qualsiasi singola azienda non subisca violazioni. In questo caso, l'incentivo di un'azienda a investire è rafforzato dalla presenza di concorrenti che intraprendono lo stesso investimento. La relazione negativa, invece, si verifica quando la proporzione di aziende che evitano le violazioni è inferiore alla probabilità iniziale, riducendo l'incentivo a investire in sicurezza.

Jianqiang et al. (2015) esaminano due aziende interdipendenti in modo simmetrico che possono effettuare un investimento continuo in sicurezza informatica. Gli autori modellano gli spillover di mercato come una perdita aggiuntiva subita da un'azienda quando questa viene colpita da un attacco informatico, mentre il concorrente no.

Calcolando il livello di investimento di equilibrio di Nash, gli autori scoprono che le aziende tendono a sovrainvestire in sicurezza quando gli spillover di mercato sono alti, per paura di perdere quote di mercato a favore dei concorrenti. Al contrario invece, quando gli spillover di mercato sono bassi le aziende tendono a sottovalutare gli investimenti in sicurezza, esponendosi dunque a maggiori rischi.

Queste conclusioni evidenziano l'importanza degli spillover di mercato nelle decisioni di investimento in sicurezza informatica e suggeriscono la necessità di politiche che bilancino gli investimenti, riducendo il rischio di sovrainvestimento o sottovalutazione della sicurezza.

Una recenente aggiunta invece di Ciet Noé e Verdier Marianne esplora nel loro articolo "Cyber Security and Cloud Outsourcing of Payments" gli incentivi di due banche concorrenti nel mercato dei prodotti per esternalizzare i loro servizi di pagamento a un'infrastruttura comune basata su cloud, gestita da un fornitore terzo privato (TPP: third privat party).

Nel modello sviluppato il fornitore di servizi cloud offre alle banche due servizi differenti: capacità di archiviazione e un'app di pagamento, ciascuno con una tariffa specifica. Le banche competono nel mercato dei depositi lungo una linea nel framework di Hotelling e offrono servizi di pagamento ai loro consumatori, la cui qualità dipende dalla sicurezza dei loro sistemi di pagamento. Se i depositanti delle banche utilizzano la stessa app di pagamento, possono inviarsi denaro reciprocamente. Alcuni depositanti sono ingenui, mentre altri sono sofisticati e scelgono le loro banche in base al livello di rischio del sistema di pagamento. Poiché le banche non possono discriminare i prezzi tra i consumatori, il prezzo dei depositi riflette la differenziazione orizzontale delle banche sulla linea di Hotelling e la differenziazione verticale in termini di sicurezza del sistema di pagamento.

Le banche decidono se unirsi o meno al cloud confrontando i benefici e i costi dell'esternalizzazione dei loro servizi di pagamento. Da un lato, se entrambe le banche si uniscono al cloud e diventano interoperabili, i loro depositanti possono godere dei benefici degli effetti di rete. Dall'altro lato, la sicurezza del loro sistema di pagamento cambia e dipende dall'investimento del fornitore di servizi cloud. Inoltre, le banche perdono i benefici della differenziazione della sicurezza, che ottengono se competono con soluzioni di pagamento indipendenti. Oltre a queste, altre inefficienze possono sorgere, quando le banche si uniscono al cloud, da danni derivanti da azzardo morale. Infatti, il fornitore di servizi cloud potrebbe sotto-riferire gli incidenti cibernetici, riducendo la capacità delle banche e dei depositanti di richiedere compensazioni.

Gli autori, attraverso l'analisi dell'ottimo sociale, dimostrano che la decisione di esternalizzare i servizi di pagamento al cloud beneficia la società solo se i benefici marginali sociali dell'interoperabilità superano i costi marginali potenziali in termini di rischio. Nell'allocazione ottimale (first best), non esiste azzardo morale, il che implica che il fornitore di servizi cloud non nasconde alcuna informazione in caso di incidente cibernetico. Gli autori mostrano che il livello di sicurezza del sistema di pagamento che massimizza il benessere sociale è maggiore se entrambe le banche si uniscono al cloud, purché il beneficio marginale di delegare gli investimenti in sicurezza a un fornitore terzo superi i costi marginali. Questo accade se il costo di investimento in sicurezza cibernetica del fornitore di servizi cloud è sufficientemente basso rispetto a quello delle banche.

Attraverso l'analisi del gioco in cui le banche decidono se unirsi al cloud dopo aver investito nella sicurezza del sistema di pagamento, gli autori dimostrano che il fornitore di servizi cloud si impegna a offrire un determinato livello di sicurezza e sceglie le tariffe di accesso e compatibilità che le banche devono pagare per esternalizzare i loro sistemi di pagamento. Quando si verifica un incidente cibernetico, il regime di responsabilità distribuisce la perdita totale tra il fornitore di servizi cloud, le banche e i depositanti. L'azzardo morale genera alcuni benefici e costi per le banche: se un incidente cibernetico non viene scoperto, le banche evitano di risarcire i depositanti, riducendo il loro costo marginale. Tuttavia, la sotto-fornitura di informazioni da parte del fornitore di servizi cloud aumenta le perdite in caso di incidente cibernetico, implicando che le banche si aspettano perdite maggiori quando decidono di unirsi al cloud.

Gli autori mostrano che in un equilibrio simmetrico, entrambe le banche esternalizzano i loro servizi di pagamento se il fornitore di servizi cloud ottiene un profitto positivo, altrimenti rimangono indipendenti. Anche se un equilibrio asimmetrico non esiste nella loro impostazione, la possibilità che una banca possa deviare dalla situazione in cui entrambe le banche si uniscono al cloud per godere dei benefici di una maggiore differenziazione della sicurezza limita la strategia di prezzo del fornitore di servizi cloud.

Contrariamente alla convinzione comune che spesso assume che le banche tendano a esternalizzare eccessivamente i loro servizi di pagamento al cloud, gli autori dimostrano che le banche possono talvolta scegliere di non esternalizzare a sufficienza rispetto alla situazione che massimizza il benessere sociale. Identificano le condizioni di mercato in cui le banche sotto-esternalizzano (o sovra-esternalizzano) i loro servizi di pagamento. Le banche tendono a scegliere livelli eccessivi di interoperabilità per ridurre la concorrenza per i depositi. Tuttavia, in questo articolo, gli autori evidenziano come il rischio cibernetico riduca gli incentivi delle banche a esternalizzare eccessivamente e possa persino portare le banche a non esternalizzare abbastanza rispetto all'ottimo sociale.

Gli autori evidenziano che la struttura di mercato verticale implica che il fornitore di servizi cloud sceglie i prezzi dopo che le banche hanno scelto i loro investimenti in sicurezza, non internalizzando l'impatto della sua strategia di prezzo sugli incentivi all'investimento delle banche. Gli incentivi all'investimento delle banche sono distorti dalla presenza di azzardo morale, anche se l'effetto finale sugli investimenti delle banche è ambiguo. Il fornitore di servizi cloud non internalizza l'impatto del danno atteso delle banche sulla concorrenza per i depositi e né le banche né il fornitore di servizi cloud internalizzano le perdite attese subite dai depositanti ingenui.

Impatto del regime di responsabilità

Concludono l'articolo analizzando come il regime di responsabilità per incidenti cibernetici impatti la sicurezza del sistema di pagamento e le decisioni di esternalizzazione delle banche. L'articolo analizza diverse opzioni normative, tra cui un regime di responsabilità per gli incidenti informatici, la supervisione degli accordi di esternalizzazione, un modello di responsabilità condivisa e la fornitura pubblica di servizi di pagamento.

Aumentare la responsabilità del fornitore di servizi cloud nei confronti dei depositanti ha un impatto maggiore sulla sicurezza del sistema di pagamento rispetto all'aumento della sua responsabilità nei confronti delle banche. Ciò suggerisce che le normative dovrebbero concentrarsi sulla protezione dei consumatori per incentivare investimenti nella sicurezza informatica.

L'articolo sottolinea che la decisione di esternalizzare o meno comporta un compromesso tra i vantaggi dell'interoperabilità e i rischi per la sicurezza. Non esiste una soluzione univoca e le decisioni ottimali dipendono da una serie di fattori specifici del mercato e del contesto normativo.

2.7 Altri contributi

Non tutti gli articoli riguardanti la cybersecurity seguono ovviamente la classificazione proposta precedentemente. Alcuni esplorano aspetti diversi e non correlati esclusivamente alle tipologie di interdipendenza tradizionali.

Uno degli articoli più significativi pubblicato recentemente, che non rientra nella classificazione proposta, è quello di Wing Man Wynne Lam e Jacob Seifert.

L'articolo esplora come le aziende scelgono le loro strategie di privacy dei dati e di sicurezza informatica sottolineando l'interdipendenza tra queste due aree e le relative implicazioni normative. Con un mercato dei dati globale valutato tra 25 e 49 miliardi di dollari, l'importanza delle decisioni aziendali riguardanti la diffusione dei dati dei consumatori è evidente. L'articolo fa distinzione tra due percorsi di diffusione: la privacy dei dati che implica accordi di condivisione volontaria, e la sicurezza informatica focalizzata sulla prevenzione degli accessi non autorizzati. Viene anche evidenziata l'importanza della regolamentazione di queste attività, facendo riferimento a casi significativi come la raccolta dei dati dei profili Facebook da parte di Cambridge Analytica e le violazioni della sicurezza che hanno interessato Facebook, Equifax e Zoom.

Gli autori sviluppano un modello che coinvolge due aziende: un controllore dei dati e una terza parte, che servono una popolazione di consumatori sofisticati e ingenui. I consumatori forniscono dati personali al controllore in cambio di un servizio, mentre la terza parte offre un servizio separato che diventa più prezioso con i dati dei consumatori. La condivisione dei dati comporta rischi di attacchi informatici, con la possibilità che i danni si ripercuotano sulla terza parte. Il modello tiene conto della responsabilità per i danni informatici, generalmente suddivisa tra aziende e consumatori.

L'articolo dimostra che la privacy e la sicurezza sono inversamente correlate, significando che gli investimenti in sicurezza tendono a essere maggiori quando i dati sono condivisi. Questa relazione nasce dagli effetti contrastanti della condivisione dei dati sugli incentivi all'investimento. Da un lato, la consapevolezza dei rischi da parte dei consumatori sofisticati riduce la domanda di condivisione dei dati, diminuendo gli incentivi agli investimenti. Dall'altro, la domanda diventa più sensibile al livello di sicurezza, incentivando maggiori investimenti per attrarre i clienti attenti alla sicurezza. Inoltre, i prezzi più bassi con la condivisione dei dati aumentano la domanda ma indeboliscono la sensibilità alla sicurezza. Di conseguenza, le aziende investono di più in sicurezza quando condividono i dati, a condizione che il danno di ogni attacco informatico sia relativamente piccolo.

L'articolo confronta l'equilibrio di mercato con un benchmark di benessere di second-best, in cui un pianificatore sociale determina la sicurezza informatica e la condivisione dei dati, lasciando i prezzi al mercato. Questo benchmark è rilevante per le normative in stile GDPR del Regno Unito, che si concentrano sulla privacy e sulla sicurezza piuttosto che sui controlli sui prezzi. L'analisi rivela fallimenti del mercato in cui le aziende sottoinvestono in sicurezza informatica e condividono eccessiva-

mente i dati, sfruttando i consumatori ingenui che non riescono a prevedere i danni informatici.

L'articolo esamina diversi interventi normativi, come gli standard minimi di sicurezza che, sebbene possano migliorare la sicurezza informatica, possono anche esacerbare i problemi di privacy se le aziende sono incentivate a condividere di più i dati per compensare i maggiori costi di sicurezza. La divulgazione e l'educazione dei consumatori possono aumentare la consapevolezza dei rischi, riducendo la condivisione eccessiva dei dati, ma potrebbero anche portare a una diminuzione degli investimenti in sicurezza poiché le aziende rispondono alla minore domanda. La responsabilità per danni completi, rendendo il controllore dei dati responsabile di tutti i danni informatici, inclusi quelli subiti dalla terza parte, può aumentare gli investimenti in sicurezza, ma potrebbe anche disincentivare la condivisione dei dati anche quando è socialmente vantaggiosa. Infine, le strategie di mitigazione dei consumatori, che consentono ai consumatori di ridurre i danni informatici attraverso misure come la modifica delle password, possono avere conseguenze ambigue. Mentre i consumatori sopportano una parte maggiore del costo della sicurezza, le aziende potrebbero investire meno in sicurezza, con conseguenti effetti potenzialmente negativi sul benessere sociale.

In conclusione, l'articolo sostiene che gli approcci normativi unilaterali spesso non riescono ad affrontare i fallimenti del mercato relativi alla privacy e alla sicurezza dei dati. Sono invece essenziali approcci coordinati che considerino l'interdipendenza tra queste scelte. Suggerisce che i futuri quadri normativi dovrebbero concentrarsi su una rigorosa supervisione delle pratiche di sicurezza informatica e potenzialmente allontanarsi dall'eccessiva dipendenza dall'autoregolamentazione.

3 Dati

In questa sezione, verranno presentati e analizzati i dati relativi alla digitalizzazione e, in particolare, alla cybersicurezza sul territorio italiano. L'obiettivo è esplorare come la realtà dei dati si relazioni con le teorie economiche e i modelli matematici illustrati nei capitoli precedenti, cercando di trarre conclusioni che possano essere utili sia a livello pratico che accademico.

Uno dei principali ostacoli nell'analisi del panorama della cybersicurezza in Italia risiede nella limitata disponibilità di dati dettagliati specialmente in relazione agli investimenti specifici in sicurezza informatica da parte delle singole aziende. Questo è dovuto al fatto che la cybersicurezza, per sua stessa natura, rappresenta un ambito estremamente sensibile e privato, e molte organizzazioni scelgono di non condividere apertamente informazioni su questa tipologia di investimenti, per ragioni legate alla riservatezza e alla protezione dei propri sistemi.

Di conseguenza, risulta complesso effettuare analisi precise che possano confermare o smentire le ipotesi teoriche e i modelli matematici trattati precedentemente, specialmente per quanto riguarda il confronto con il cosiddetto "ottimo sociale" o con il livello di investimento socialmente efficiente. Questi concetti sono infatti di natura astratta e richiederebbero dati dettagliati sugli investimenti aziendali che non sono sempre disponibili.

Nonostante queste limitazioni la presente sezione si propone di fare il miglior uso possibile dei dati disponibili e delle informazioni pubbliche, con l'obiettivo di trarre considerazioni utili su alcune delle principali tematiche legate alla cybersicurezza in Italia. Tra i dati disponibili vi sono quelli relativi agli attacchi informatici subiti dalle aziende italiane, le contromisure adottate comunemente e i livelli di sicurezza riscontrati nei diversi settori economici. L'analisi di questi dati permetterà di riflettere sulle dinamiche di sicurezza informatica nel nostro paese, cercando di collegare tali evidenze empiriche alle teorie e ai modelli esplorati in precedenza.

Il primo passo sarà utilizzare gli indicatori e i dati disponibili per catalogare i vari settori economici italiani in base a due dimensioni chiave: l'interdipendenza tecnica e l'interdipendenza di mercato, due concetti centrali della letteratura sulla sicurezza informatica. Questi concetti consentiranno di suddividere i settori in categorie che rispecchiano, in modo approssimativo, le tipologie di interdipendenza studiate nei modelli teorici.

Successivamente, verranno presentati i risultati delle analisi relative alle violazioni informatiche registrate e ai livelli generali di sicurezza nei diversi settori. Ci si concentrerà quindi su un confronto tra i settori appartenenti alle diverse categorie di interdipendenza, cercando di individuare pattern ricorrenti e particolari vulnerabilità legate a specifici contesti di mercato o reti informatiche comuni.

3.1 Presentazione dei dati

Il Rapporto ICT nelle Imprese, viene stilato annualmente dall'ISTAT, la prima edizione risale al 2007 per arrivare ad oggi fino al 2023 e fornisce una panoramica aggiornata sull'adozione delle tecnologie dell'informazione e della comunicazione (ICT) nelle imprese italiane. Questo report viene rivisto e perfezionato ogni anno, introducendo nuovi indicatori o aggiornando quelli esistenti per riflettere le evoluzioni tecnologiche e i cambiamenti strutturali del tessuto imprenditoriale. Ogni edizione, quindi, rappresenta uno spaccato aggiornato dello stato della digitalizzazione, includendo variazioni o nuove metriche, se necessarie.

Il rapporto raccoglie dati sull'uso delle tecnologie digitali da parte delle imprese italiane, analizzando aspetti come la digitalizzazione dei processi, l'adozione di tecnologie avanzate, l'uso del cloud computing e il livello di cybersicurezza. Coprendo diversi settori economici e permettettendo di confrontare l'adozione delle tecnologie tra piccole, medie e grandi imprese evidenziando le tendenze emergenti nel panorama nazionale.

3.2 Struttura dei Dati

I dati analizzati nel presente report, stilato annualmente, sono organizzati principalmente sulla base della dimensione delle imprese, con una suddivisione in quattro categorie principali:

- **Micro imprese**: con un numero di dipendenti compreso tra 10 e 49.
- **Piccole imprese**: con un numero di dipendenti compreso tra 50 e 99.
- **Medie imprese**: con un numero di dipendenti compreso tra 100 e 249.
- **Grandi imprese**: con oltre 250 dipendenti.
- **Tutte**: da 0 a oltre 250 dipendenti.

Questa suddivisione è fondamentale per comprendere le differenze nelle dotazioni tecnologiche, nelle strategie di cybersicurezza e nelle risposte agli attacchi informatici in base alla scala dimensionale delle aziende.

Ogni gruppo di imprese, suddiviso per dimensione, viene poi ulteriormente classificato in base a determinati codici **ATECO**, che identificano il settore economico di appartenenza. Nella tabella seguente verranno riportati i principali codici ATECO analizzati per le imprese di ciascuna categoria dimensionale.

Inoltre, per ciascun gruppo di imprese e settore di appartenenza, sono definiti una serie di **indicatori**, che permettono di analizzare vari aspetti relativi alla digitalizzazione e alla cybersicurezza. Questi indicatori possono variare di anno in anno, poiché il report viene aggiornato periodicamente per includere nuovi parametri o per adattare le misurazioni alle necessità emergenti.

Settori economici e codici ATECO

Il dataset copre una vasta gamma di settori economici italiani classificati secondo la codifica ATECO del 2007. Questi settori includono principalmente attività manifatturiere, servizi di supporto alle imprese, attività legate all'energia e alla gestione dei rifiuti, commercio, telecomunicazioni, e altro ancora. Ogni settore è suddiviso ulteriormente in specifiche categorie che facilitano la classificazione delle imprese in base al tipo di attività economica svolta.

Di seguito è fornita una lista dettagliata dei settori con i rispettivi codici ATECO trattati nel dataset:

Macro Categoria	**Sotto-categoria**
C Attività manifatturiere	CA Industrie alimentari, delle bevande e del tabacco CB Industrie tessili, dell'abbigliamento, articoli in pelle e simili CC Industria dei prodotti in legno e carta, stampa CD-CG Fabbricazione di coke, prodotti chimici, farmaceutici, gomma, plastica e minerali non metalliferi CH Metallurgia e fabbricazione di prodotti in metallo esclusi macchinari e attrezzature 26 Fabbricazione di computer, prodotti elettronici e ottici, apparecchi elettromedicali e di misurazione CJ-CK Fabbricazione di apparecchiature elettriche, domestiche e macchinari CL Fabbricazione di mezzi di trasporto CM Altre industrie manifatturiere, riparazione e installazione di macchine e apparecchiature
D-E Fornitura di energia elettrica, gas, vapore e gestione rifiuti	0036 Fornitura di energia elettrica, gas, vapore, aria condizionata, acqua, gestione dei rifiuti e risanamento
F Costruzioni	

G Commercio all'ingrosso e al dettaglio	47 Commercio al dettaglio (escluso autoveicoli e motocicli)
H Trasporto e magazzinaggio	0049 Trasporto e magazzinaggio (esclusi servizi postali e corrieri) 53 Servizi postali e attività di corriere
I Alloggio e ristorazione	55 Alloggio 56 Attività dei servizi di ristorazione
J Servizi di informazione e comunicazione	JA_X_58 Attività di produzione audiovisiva 58 Attività editoriali 61 Telecomunicazioni JC Informatica ed altri servizi d'informazione
L Attività immobiliari	68 Attività immobiliari
M Attività professionali, scientifiche e tecniche	
N Noleggio, agenzie di viaggio, supporto alle imprese	0032 Noleggio, agenzie di viaggio e servizi di supporto alle imprese (escluso agenzie di viaggio e tour operator) 79 Attività dei servizi delle agenzie di viaggio, tour operator e servizi di prenotazione
0033 Settore ICT	
0034_B Servizi non finanziari	Totale servizi non finanziari (G-N, incluso 951, escluso K)
0035_B Totale attività economiche	Totale attività economiche (C-N, incluso 951, escluso K)

Tabella 3.1: Codici ATECO e struttura gerarchica delle categorie

Suddivisione del report

Il report sulla digitalizzazione delle imprese italiane e sull'adozione delle tecnologie ICT è suddiviso in diverse aree tematiche, ciascuna delle quali analizza specifici aspetti dell'innovazione tecnologica e della gestione aziendale. Questi ambiti tematici coprono sia l'uso delle tecnologie nelle operazioni quotidiane delle imprese, sia l'implementazione di soluzioni avanzate per migliorare la competitività e la sicurezza informatica.

Le principali sezioni del report sono le seguenti:

- **Principali indicatori**: Raccolta degli indicatori chiave che riassumono lo stato della digitalizzazione nelle imprese.
- **Vendite on-line**: Indicatori che analizzano la diffusione e l'importanza delle vendite online tra le imprese.
- **Cloud Computing**: Sezione dedicata all'adozione di soluzioni di cloud computing, con informazioni su come queste tecnologie vengono utilizzate dalle imprese.
- **Competenze e formazione in ICT**: Indicatori che misurano il livello di competenza e la formazione del personale nell'uso delle tecnologie digitali.
- **Indicatori Industria 4.0 - Fattori di digitalizzazione**: Dati che riguardano l'adozione di soluzioni dell'Industria 4.0 per migliorare la produttività e l'efficienza.
- **Intelligenza Artificiale**: Sezione che tratta l'uso di sistemi di intelligenza artificiale nelle aziende.
- **Connessione e utilizzo di Internet, sito web**: Analisi della connettività delle imprese, inclusa la presenza online e l'utilizzo di servizi web.
- **Social Media**: Dati relativi all'uso dei social media da parte delle imprese per scopi di marketing e comunicazione.
- **Acquisti on-line**: Misura la diffusione degli acquisti online di beni e servizi tra le imprese.
- **Robotica e stampa 3D**: Indicatori sull'adozione di tecnologie robotiche e di stampa 3D nell'ambito manifatturiero.
- **ICT e ambiente**: Sezione dedicata all'impatto delle tecnologie ICT sulle pratiche sostenibili e ambientali.
- **Indicatori DESI**: Misurazione di vari indicatori che fanno parte del Digital Economy and Society Index (DESI) a livello nazionale.

- **Sicurezza informatica**: Indicatori relativi alle pratiche di sicurezza informatica e alle contromisure adottate dalle imprese.
- **Fatturazione elettronica**: Diffusione e utilizzo della fatturazione elettronica come strumento di digitalizzazione dei processi amministrativi.
- **ICT nelle imprese - Ripartizioni territoriali**: Sezione che fornisce dati dettagliati sull'adozione dell'ICT in diverse aree geografiche del paese.
- **Tecnologie per l'organizzazione interna, di filiera e Internet delle cose**: Indicatori relativi all'adozione di tecnologie per la gestione interna, per la supply chain e per l'Internet of Things (IoT).
- **Analisi di Big Data**: Sezione che tratta l'uso dei Big Data per prendere decisioni strategiche all'interno delle imprese.

È importante notare che gli indicatori presenti nel report non appartengono necessariamente ad una sola delle categorie tematiche elencate in precedenza. Alcuni indicatori, infatti, possono essere rilevanti per più di una categoria e riportati in diverse sezioni del report. Ad esempio, un indicatore relativo alla "sicurezza informatica" potrebbe essere presente sia nella sezione dedicata alla "sicurezza informatica" che in quella relativa alle "tecnologie per l'organizzazione interna", poiché la sua applicabilità si estende a più ambiti aziendali. Inoltre, dato che il report viene stilato annualmente con dati nuovi, e gli indicatori sono in continua evoluzione, è difficile fornire una lista precisa di quelli presenti in tutti gli anni. Per le analisi, è stato quindi effettuato un lavoro di sintesi, selezionando solo gli indicatori comuni a tutto il periodo che abbiamo deciso di analizzare. Questi verranno illustrati nel dettaglio nelle sezioni specifiche dedicate all'analisi.

3.3 Classificazione dei settori

In questa sezione ci dedicheremo a una prima analisi degli indicatori presenti nel dataset, con lo scopo di classificare i codici ATECO e, quindi, i settori delle aziende in Italia secondo la suddivisione proposta dalla letteratura sugli investimenti in cybersicurezza.

Gli articoli esaminati distinguono le aziende secondo due tipologie di interdipendenze: interdipendenze di mercato e interdipendenze tecniche.

Interdipendenze di mercato

Le interdipendenze di mercato sono caratterizzate da un contesto di business stealing, in cui i clienti possono facilmente migrare da un'azienda all'altra in seguito a un attacco informatico. Questa dinamicità porta le aziende a investire in cybersicurezza in modo eccessivo rispetto a quello che sarebbe socialmente ottimale, cercando di proteggere i propri clienti da potenziali attacchi e dai competitor.

Interdipendenze tecniche

Le interdipendenze tecniche, invece, fanno riferimento a imprese che condividono infrastrutture e sistemi informatici, operando su piattaforme comuni. In caso di attacco informatico, queste aziende sono esposte al rischio di contagio, con un possibile effetto a catena. Questo fenomeno induce un comportamento di free riding, dove le aziende investono meno in cybersicurezza rispetto al livello socialmente desiderabile, confidando che siano altre aziende del network a sostenere i costi maggiori per la protezione comune.

Classificazione degli indicatori

Per classificare le aziende lungo questi due assi (interdipendenze di mercato e tecniche), sono stati selezionati gli indicatori del dataset che si ritenevano più appropriati per fornire una classificazione coerente. Si è utilizzata l'edizione del 2023 del dataset, poiché in questo contesto i dati più recenti e dettagliati si sono rivelati utili per catturare al meglio la struttura e le dinamiche delle imprese. Le seguenti categorie di indicatori sono state analizzate:

- Commercio elettronico
- Vendite online
- Cloud computing
- Indicatori DESI
- Industria 4.0
- Competenze e formazione
- Tecnologie per l'organizzazione interna, di filiera e internet delle cose

Gli indicatori aggiornati al 2023 e utilizzati per questa analisi sono i seguenti:

Commercio elettronico

- Vendita on-line via web e/o sistemi di tipo EDI
- Per valori almeno uguali all'1% del fatturato totale
- Via web
- Via sistemi di tipo EDI
- Vendita via web a clienti finali (B2C) (incidenza % su imprese che vendono via web)
- Vendita via web ad altre imprese o pubbliche amministrazioni (B2B o B2G) (incidenza % su imprese che vendono via web)
- Vendite via web tramite siti web o app dell'impresa

- Vendite via web tramite siti web o app di intermediari
- Vendite via web tramite siti web o app di intermediari per almeno il 50% del valore delle vendite via web
- Vendite via web tramite siti web o app di intermediari per almeno il 20% del valore delle vendite via web

Vendita online

- Quota maggiore o uguale all'1%
- Quota maggiore o uguale al 2%
- Quota maggiore o uguale al 5%
- Quota maggiore o uguale al 10%
- Quota maggiore o uguale al 25%
- Quota maggiore o uguale al 50%
- Valore delle vendite on-line (via web e via EDI, al netto dell'IVA) (incidenza % sul valore totale delle vendite)

Cloud computing

- Posta elettronica
- Software per ufficio
- Archiviazione di file
- Hosting di database dell'impresa
- Applicazioni software di finanza e contabilità
- Applicazioni software di customer relationship management
- Potenza di calcolo per eseguire il software dell'impresa
- Imprese che acquistano almeno uno dei servizi di cloud computing richiesti
- Applicazioni software ERP
- Applicazioni software di sicurezza informatica
- Piattaforma informatica per lo sviluppo, il test e la distribuzione di applicazioni
- Imprese che acquistano servizi di cloud computing di livello base (incidenza %)
- Imprese che acquistano servizi di cloud computing di livello intermedio (incidenza %)

- Imprese che acquistano servizi di cloud computing di livello sofisticato (incidenza %)

Competenze e formazione

- Imprese che impiegano specialisti ICT (incidenza %)
- Imprese che nell'anno precedente hanno assunto o provato ad assumere personale con competenze specialistiche in ICT (incidenza %)
- Con difficoltà a ricoprire i posti vacanti (incidenza %)
- Imprese che hanno organizzato corsi di formazione per sviluppare o aggiornare le competenze ICT/IT (incidenza %)
- Corsi destinati ad addetti con competenze specialistiche in ICT (incidenza %)
- Corsi destinati ad addetti senza competenze specialistiche in ICT/IT (incidenza %)
- Funzioni ICT svolte da personale interno all'impresa o al gruppo (incidenza %)
- Funzioni ICT svolte da personale esterno (incidenza %)

Industria 4.0 - Aree tecnologie di acquisto

- Area Internet delle cose (IoT)
- Area stampa 3D
- Area robotica
- Area cloud computing
- Area applicazioni web o app
- Area vendite online
- Area social media
- Area Big Data Analytics
- Area realtà aumentata e realtà virtuale
- Area sicurezza informatica
- Altre aree per lo sviluppo tecnologico
- Imprese che ritengono non importanti le aree tecnologiche per il proprio sviluppo (incidenza %)
- Imprese che non sanno rispondere (incidenza %)

Indicatori DESI

- PMI (10-249 addetti) che hanno effettuato vendite online per valori almeno uguali all'1% del fatturato totale (incidenza % sul totale PMI)
- Valore del fatturato online delle PMI (incidenza % sul totale fatturato PMI)
- Imprese con un livello base di digitalizzazione
- Imprese che acquistano servizi di cloud computing di livello intermedio o sofisticato (incidenza %)

Tecnologie per l'organizzazione interna, di filiera e internet delle cose

- Imprese che usano software CRM (incidenza %)
- Imprese che usano software BI (incidenza %)
- Imprese che usano almeno un software gestionale (ERP, CRM, BI) (incidenza %)
- Imprese che condividono in rete con fornitori e clienti dati sulla gestione della catena distributiva (SCM) (incidenza %)
- Imprese con sistemi ERP per condividere informazioni tra differenti aree funzionali (incidenza %)

Scelta degli indicatori per l'analisi

A partire da questa lista, sono stati selezionati gli indicatori più rappresentativi per la caratterizzazione delle aziende secondo l'asse dell'interdipendenza di mercato e di quella tecnica.

Interdipendenza di mercato

Come discusso in precedenza, l'interdipendenza di mercato è caratterizzata dalla facilità con cui i clienti possono migrare da un'azienda all'altra in caso di attacco informatico. Per modellare questa facilità di transizione, l'indicatore più appropriato è risultato essere la quota delle vendite online. La presenza sul web rende infatti le aziende meno differenziate e più facili da sostituire per i clienti, riducendo le barriere di cambio tra un'impresa e un'altra.

Un altro indicatore rilevante è la quantità di dati analizzati internamente sui clienti. Questo indicatore accompagna il precedente, poiché le aziende che investono nell'analisi dei dati sui clienti tendono a operare in contesti fortemente competitivi, dove la differenziazione tra imprese è bassa e la pressione competitiva elevata. In questo caso, la raccolta e l'analisi dei dati sui clienti dimostrano che l'azienda partecipa attivamente a un mercato competitivo, dove l'interdipendenza di mercato è forte.

Interdipendenza tecnica

Per quanto riguarda l'interdipendenza tecnica, gli indicatori principali utilizzati come proxy della partecipazione a network comuni sono stati:

Vendite tramite siti web o app esterni, che indicano una forte dipendenza da piattaforme condivise; Condivisione dei dati della catena distributiva (SCM) con fornitori e clienti, che evidenzia la cooperazione su sistemi informatici comuni; Hosting di database e utilizzo di servizi di cloud computing, che segnalano un'adesione a infrastrutture IT condivise. Combinando questi indicatori, si è costruita una rappresentazione accurata del livello di interdipendenza tecnica, utile per classificare le aziende in funzione del loro utilizzo di piattaforme e servizi comuni all'interno del mercato.

Andando a calcolare, a media pesata degli indicatori per ognuna delle due categorie e poi assegnando i valori di una come asse x e della'altro come asse y ad ogni codice ateco possiamo graficare questi punti risultando nel seguente grafico :

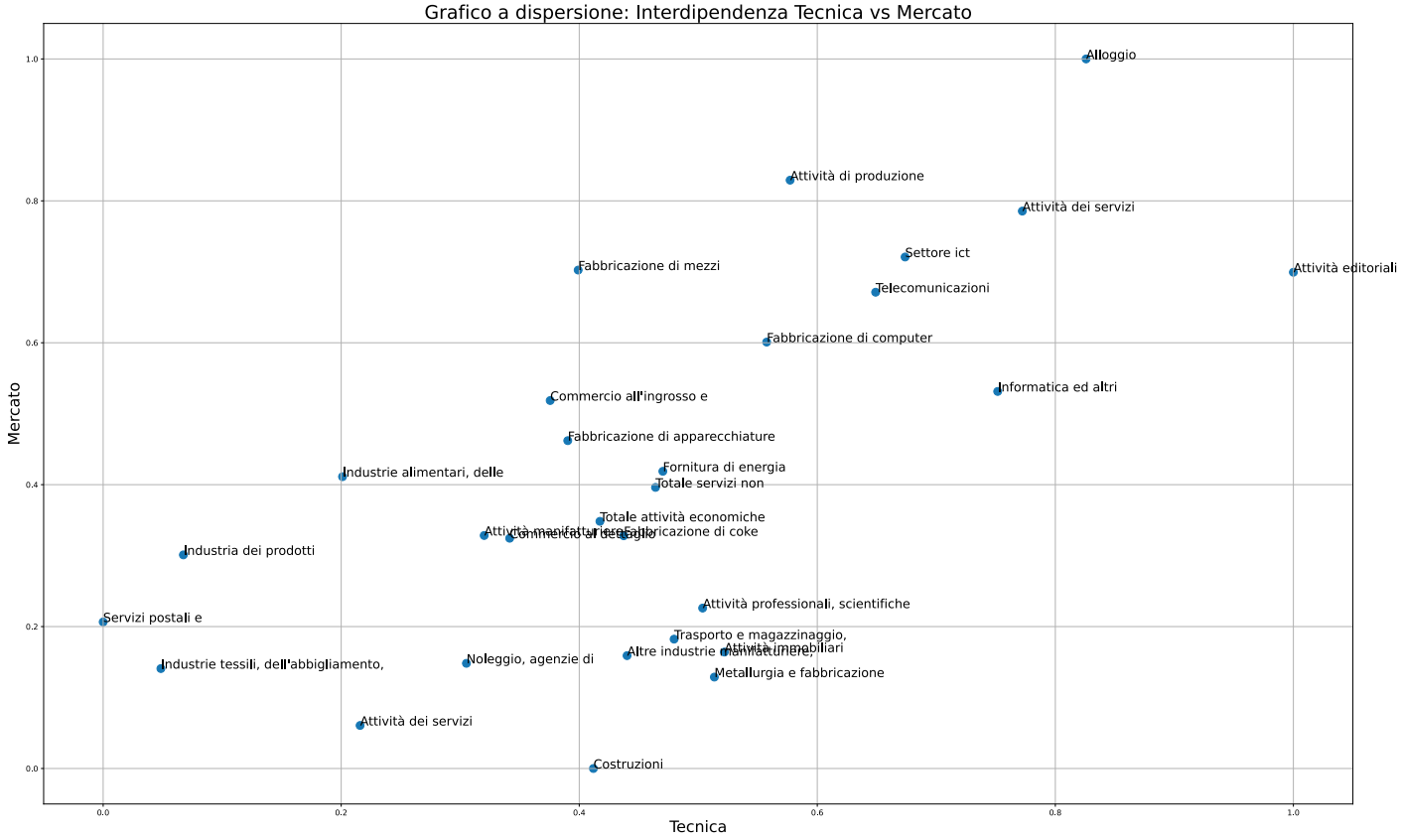

Figura 3.1

Il grafico che mostra la relazione tra interdipendenza tecnica e di mercato per i vari settori delle aziende italiane fornisce una rappresentazione piuttosto coerente con le aspettative basate sulla letteratura. Settori come telecomunicazioni, ICT e fabbricazione di computer si trovano in alto a destra, dove ci aspetteremmo di vedere industrie fortemente interconnesse sia dal punto di vista tecnico (condivisione di reti, standard comuni) sia da quello del mercato (competizione elevata e facilità per i clienti di migrare tra aziende). Questi risultati sono perfettamente in linea con la teoria che i settori digitali e tecnologici tendono a mostrare forti interdipendenze.

Un altro punto interessante è la fabbricazione di mezzi di trasporto e il commercio all'ingrosso e al dettaglio, che si collocano a metà del grafico, segnalando una moderata interdipendenza. Questo ha senso, poiché sebbene non siano settori ad alta condivisione tecnica come l'ICT, possono comunque essere influenzati da reti logistiche e sistemi digitali per la gestione della produzione e delle vendite.

Tuttavia, ci sono alcune anomalie che meritano attenzione. Ad esempio, il settore degli alloggi si trova in una posizione inaspettatamente alta rispetto all'interdipendenza di mercato e tecnica. Una possibile spiegazione potrebbe risiedere nell'uso crescente di piattaforme online per prenotazioni e gestione del flusso di clienti (come Airbnb e Booking), che porta gli alloggi a dipendere fortemente da infrastrutture esterne e a dover affrontare una concorrenza diretta online. Questo potrebbe giustificare il posizionamento, anche se non si allinea perfettamente con l'idea tradizionale del settore alberghiero.

Altre osservazioni riguardano settori come noleggio e agenzie di viaggio, che appaiono sorprendentemente in basso. Ci si aspetterebbe che il mercato dei viaggi e del noleggio, soprattutto nell'era digitale, mostri una maggiore interdipendenza di mercato, vista la forte competizione tra piattaforme e l'uso diffuso del web per l'acquisto di tali servizi. Un posizionamento più alto sarebbe atteso, e questa discrepanza potrebbe indicare una sottovalutazione dell'effetto della competizione digitale in questi settori.

In generale, la classificazione e i risultati sono validi per la maggior parte dei settori, ma riconosciamo alcune limitazioni. Alcune categorie potrebbero essere state influenzate da fattori non catturati pienamente dagli indicatori scelti. Tuttavia, queste anomalie non invalidano l'utilità del modello, che rappresenta un quadro generale abbastanza coerente con la teoria.

3.4 Dati sulla Cybersecurity

In questa sezione analizzeremo i dati relativi esclusivamente alla cybersecurity in Italia.

Come descritto in precedenza, i dati sono organizzati per anno e suddivisi in base alla dimensione delle imprese: micro, piccole, medie e grandi. Per ciascuna di queste categorie dimensionali, vengono forniti specifici indicatori relativi alla cybersecurity.

È importante notare che, all'interno di ogni anno, gli indicatori rimangono costanti per tutte le dimensioni aziendali e per ogni codice ATECO. Tuttavia, nel corso degli

anni, gli indicatori possono variare in modo significativo, soprattutto nel campo della cybersecurity, un'area relativamente nuova per le imprese italiane e in continua evoluzione. Questi cambiamenti riflettono non solo le nuove tipologie di attacchi, ma anche l'adozione di contromisure sempre più avanzate.

Nelle sezioni seguenti, esploreremo i cambiamenti negli indicatori nel tempo, analizzando come le aziende italiane abbiano reagito a queste nuove sfide di sicurezza informatica, con particolare attenzione alle evoluzioni nelle minacce e nelle strategie di difesa adottate.

Metodologia

L'obiettivo principale di questa analisi non è solo fornire uno spaccato dello stato della cybersecurity in un singolo anno, ma anche cercare di ricostruire un andamento temporale dei principali trend. In questo modo, è possibile confrontare le azioni intraprese dalle imprese e valutare l'impatto di tali interventi sull'evoluzione degli indicatori.

Il primo passo di questa analisi è stato quindi la costruzione di un panel di dati che coprisse più anni possibile, così da ottenere una visione d'insieme dell'evoluzione della cybersecurity in Italia.

Essendo questo ambito di raccolta dati relativamente nuovo, il dataset più vecchio risale solo al 2015. Successivamente, nuovi report sono stati pubblicati nel 2019 e nel 2022. Tuttavia, non tutti gli indicatori sono presenti in ciascun anno, rendendo necessario un lavoro di confronto e unione per identificare quelli comuni a più annualità.

Il processo di costruzione del panel ha richiesto l'identificazione manuale degli indicatori e la loro normalizzazione, poiché alcuni cambiavano nome da un anno all'altro pur mantenendo lo stesso significato. Questo ha permesso di unificare i nomi e gli indicatori, rendendo il dataset omogeneo per l'analisi.

Gli indicatori disponibili dal 2015 al 2022 sono:

- Incidenza degli attacchi hacker, suddivisi per:
  - Distruzione o corruzione dei dati
  - Divulgazione dei dati
  - Indisponibilità dei servizi ICT causata dall'attacco
  - Media totale degli attacchi

Oltre a questi, per gli anni 2019 e 2022 sono stati aggiunti i seguenti indicatori:

- Consapevolezza sulla sicurezza ICT tra i dipendenti:
  - Consapevolezza volontaria
  - Consapevolezza obbligatoria
  - Consapevolezza per contratto

- Confronto tra sicurezza gestita internamente o esternamente:
  - Sicurezza ICT interna
  - Sicurezza ICT esterna
- Adozione di misure di sicurezza:
  - Password
  - Backup dei dati
  - Autenticazione biometrica
  - Crittografia
  - Controllo di accesso di rete
  - VPN aziendale
  - File di registro
  - Valutazione interna del rischio ICT
  - Test di penetrazione/sicurezza ICT

Un'altra peculiarità del dataset è che gli indicatori relativi alla cybersecurity sono disponibili per tutti i codici ATECO elencati in precedenza, ma solo per il livello aggregato delle imprese con 10 o più dipendenti. In altre parole, i dati a livello aggregato non distinguono tra le dimensioni aziendali, ma rappresentano un insieme di imprese con un minimo di 10 dipendenti.

Per quanto riguarda invece le imprese suddivise in micro, piccole, medie e grandi, gli indicatori sono disponibili solo per alcune macro categorie ATECO, che includono:

- Attività manifatturiere (C)
- Fornitura di energia elettrica, gas, vapore e aria condizionata, gestione dei rifiuti e risanamento (D-E)
- Costruzioni (F)
- Totale servizi non finanziari (G-N, incluso 951, escluso 75 e K)
- Totale attività economiche (C-N, inclusa 951, escluse 75 e K)

In conclusione, il risultato di questa fase iniziale di elaborazione dei dati ha portato alla creazione di 5 nuovi dataset panel:

- Un primo dataset, il più completo, che aggrega i dati per tutte le imprese con 10 o più dipendenti e include gli indicatori per tutti i codici ATECO disponibili.
- Quattro sotto-dataset che esplorano l'evoluzione degli indicatori in base alle dimensioni delle imprese (micro, piccole, medie e grandi) ma limitati alle 5 macro categorie ATECO sopra menzionate.

Questa suddivisione consente un'analisi dettagliata dell'evoluzione della cybersecurity nell'intero panorama delle imprese italiane, nonché un approfondimento su come tali evoluzioni si manifestano nelle diverse categorie dimensionali per le specifiche attività economiche.

3.4.1 Analisi dei dati relativi alla cybersicurezza per aziende con 10 e più dipendenti

Una volta costruito il panel, possiamo iniziare a esplorare i dati e identificare i principali trend che emergono. In questa fase, l'obiettivo sarà di concentrasi su un'analisi aggregata, cioè esaminando i dati relativi a tutti i settori, senza distinzione tra i vari codici ATECO. Questo per ottenere una visione d'insieme dell'evoluzione degli attacchi informatici in Italia.

Nello specifico ci concentreremo sull'incidenza degli attacchi informatici per l'intero periodo disponibile, ossia tra il 2015 e il 2022. L'aggregazione di questi dati consente di individuare eventuali cambiamenti significativi nelle minacce e nelle risposte delle imprese nel corso del tempo.

Il grafico riportato di seguito rappresenta l'incidenza percentuale di tutti gli incidenti di sicurezza informatica su base annua, misurata in termini di percentuale di imprese che hanno subito almeno un attacco (includendo indisponibilità dei servizi ICT, distruzione o corruzione di dati, e divulgazione di dati riservati).

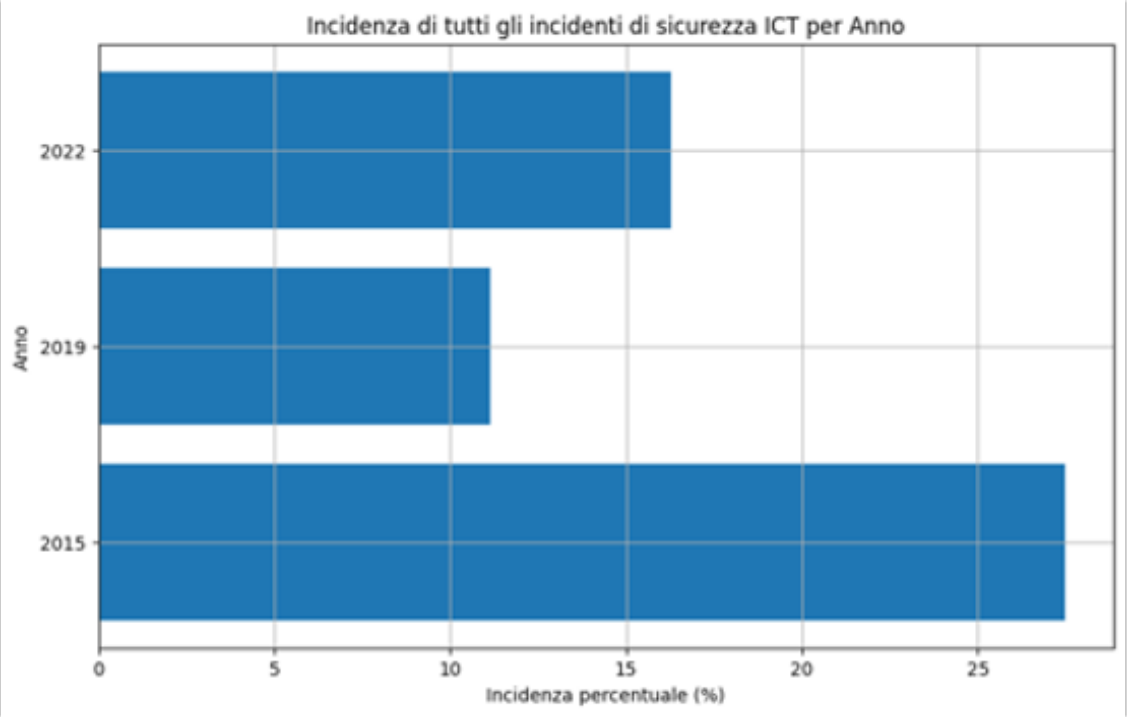

Figura 3.2: Trend generale degli attacchi dal 2015 al 2022

Osservando il grafico, possiamo notare che l'incidenza degli attacchi informatici era significativamente più alta nel 2015, quando circa il 28% delle imprese ha dichiarato di aver subito almeno un attacco informatico. Nel 2019, questa incidenza è diminuita sensibilmente, arrivando a circa il 11%. Tuttavia, nel 2022 si osserva un nuovo incremento, con un ritorno a percentuali superiori al 17%.

Questa variazione può essere spiegata da diversi fattori. Da un lato, la diminuzione tra il 2015 e il 2019 potrebbe riflettere una maggiore attenzione delle imprese verso la sicurezza informatica, con l'introduzione di misure più efficaci di prevenzione e difesa. Dall'altro, l'aumento osservato nel 2022 può essere attribuito a un ambiente tecnologico in rapida evoluzione, caratterizzato da nuove vulnerabilità legate alla crescente digitalizzazione e all'utilizzo di tecnologie emergenti, come il cloud computing e l'Internet of Things.

Inoltre, la pandemia del COVID-19 ha costretto molte aziende a riorganizzarsi rapidamente adottando soluzioni di lavoro a distanza e accelerando la trasformazione digitale. Questo potrebbe aver esposto le imprese a nuove minacce, soprattutto in un contesto in cui la sicurezza informatica non era ancora stata pienamente integrata nelle strategie aziendali.

L'andamento generale suggerisce, quindi, che le aziende devono continuare a rafforzare le loro capacità di protezione e difesa per far fronte a un panorama di minacce sempre più complesso e in evoluzione.

3.4.2 Settori più colpiti negli anni

Dopo aver analizzato l'andamento generale degli attacchi informatici, è utile approfondire quali settori specifici siano stati maggiormente colpiti nel corso degli anni. Questo ci permette di capire meglio come si distribuiscono le minacce in base alle attività economiche, e come diversi settori abbiano affrontato le sfide legate alla cybersecurity.

Analizziamo ora i dati relativi ai settori più colpiti dagli attacchi nel 2015, 2019 e 2022, identificando eventuali cambiamenti nella distribuzione degli attacchi.

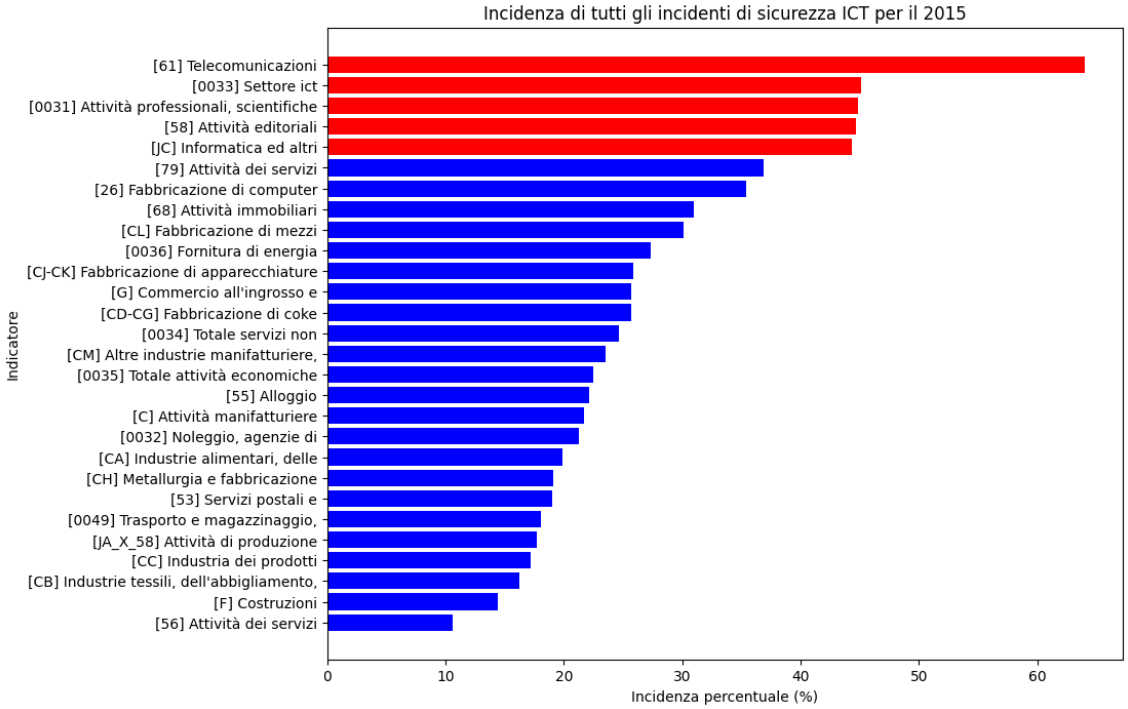

Figura 3.3: Settori più colpiti nel 2015

Nel 2015, i cinque settori più colpiti erano:

- Telecomunicazioni: 70%
- Settore ICT: 48%
- Attività professionali: 47%
- Attività editoriali: 46.5%
- Informatica: 46%

Il settore delle telecomunicazioni è stato chiaramente il più esposto agli attacchi, con un'incidenza molto più alta rispetto agli altri. Questo potrebbe essere dovuto alla sua natura di infrastruttura critica, che la rende un obiettivo privilegiato per i cybercriminali. Settori come l'ICT, l'informatica e le attività professionali, pur non avendo lo stesso livello di esposizione, dimostrano comunque una significativa vulnerabilità.

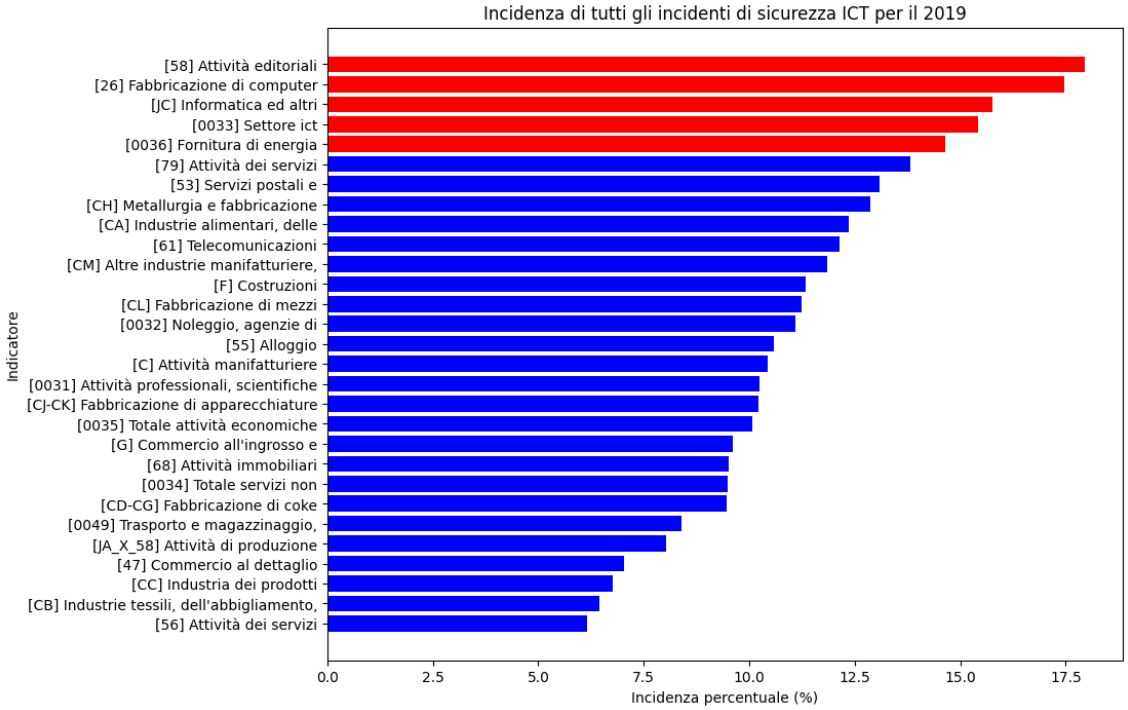

Figura 3.4: Settori più colpiti nel 2019

Nel 2019, i settori più colpiti sono leggermente cambiati:

- Attività editoriali: 18%
- Fabbricazione di computer: 17.5%
- Informatica: 16%
- Settore ICT: 15.5%
- Fornitura di energia: 14.5%

Nel 2019, si nota una significativa riduzione della percentuale di attacchi nel settore delle telecomunicazioni, sostituito dalle attività editoriali come settore più colpito. Questo cambio potrebbe riflettere una variazione nelle tecniche e nei bersagli degli attacchi informatici, con una maggiore attenzione rivolta ai settori legati all'informazione e alla gestione dei dati, probabilmente a causa della crescente importanza della privacy e della protezione dei dati personali.

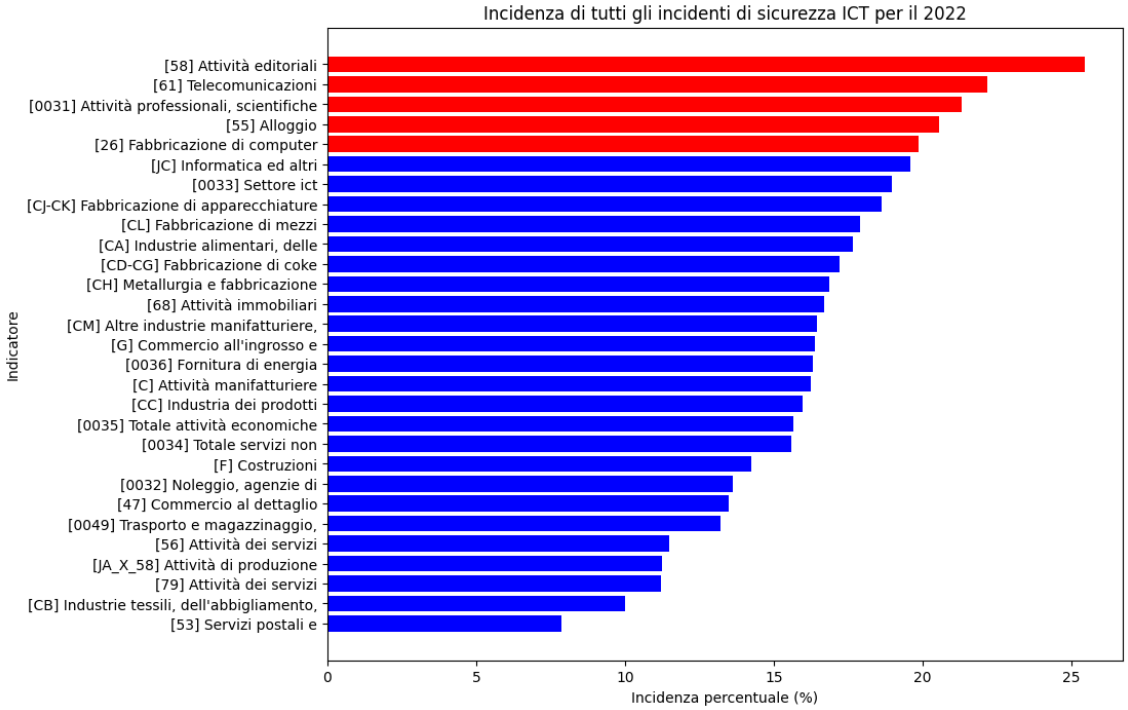

Figura 3.5: Settori più colpiti nel 2022

Nel 2022, i settori più colpiti sono stati:

- Telecomunicazioni: 22%
- Attività professionali: 20%
- Alloggio: 20%
- Fabbricazione di computer: 19%
- Attività editoriali: 16%

Nel 2022, il settore delle telecomunicazioni ritorna in cima alla lista, ma questa volta con un'incidenza più contenuta rispetto al 2015. È interessante notare anche la crescita del settore dell'alloggio tra i più colpiti, probabilmente a causa della crescente digitalizzazione e dell'uso di piattaforme online per le prenotazioni, che ha reso questo settore più vulnerabile agli attacchi. Anche le attività professionali e la fabbricazione di computer si confermano tra i settori più esposti, a riprova della continua attenzione che i cybercriminali rivolgono ai settori legati alla tecnologia e ai servizi professionali.

3.4.3 Consapevolezza e misure di sicurezza

Dopo aver analizzato gli attacchi, è importante comprendere come le aziende abbiano sviluppato le misure di sicurezza e la consapevolezza dei dipendenti nel corso degli anni. La sicurezza informatica non si limita alla reazione agli attacchi, ma richiede un approccio proattivo, che coinvolga sia l'utilizzo di strumenti di protezione avanzati sia l'incremento della consapevolezza tra i dipendenti.

Nei grafici seguenti, è possibile osservare un confronto tra la consapevolezza dei dipendenti in materia di sicurezza ICT e la gestione della sicurezza informatica, interna ed esterna, tra il 2019 e il 2022.

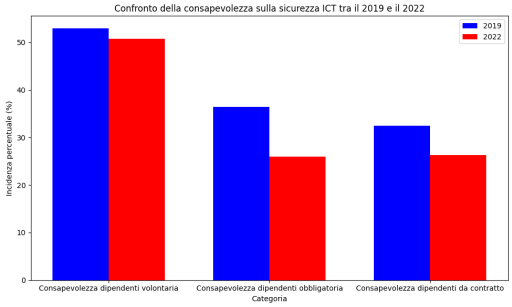

Figura 3.6: Confronto consapevolezza ICT 2019 vs 2022

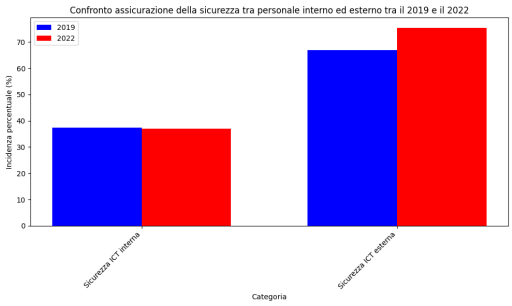

Figura 3.7: Confronto sicurezza interna vs esterna 2019 vs 2022

Nel primo grafico, vediamo come la consapevolezza dei dipendenti riguardo alla sicurezza ICT sia diminuita dal 2019 al 2022 in tutte le categorie analizzate: consapevolezza volontaria, obbligatoria e da contratto. Questo calo può essere interpretato come un segnale della crescente complessità del panorama informatico, che rende più difficile mantenere elevati livelli di attenzione tra i dipendenti.

Il secondo grafico evidenzia un cambio significativo nella gestione della sicurezza interna ed esterna. Si osserva una stabilità nella sicurezza gestita da personale interno, ma una crescita sostanziale nella scelta di affidare la sicurezza ICT a personale esterno. Questo trend potrebbe riflettere la crescente difficoltà per le aziende nel gestire autonomamente un'infrastruttura di sicurezza efficace, spingendole a rivolgersi a fornitori specializzati in grado di fornire soluzioni avanzate e aggiornate.

In sintesi, nonostante una leggera diminuzione della consapevolezza interna, le aziende stanno adottando una strategia di outsourcing della sicurezza per fronteggiare le minacce sempre più complesse.

Un altro aspetto da considerare, accanto all'esternalizzazione della gestione della sicurezza informatica, è la crescente tendenza delle aziende a sottoscrivere polizze assicurative contro gli attacchi informatici.

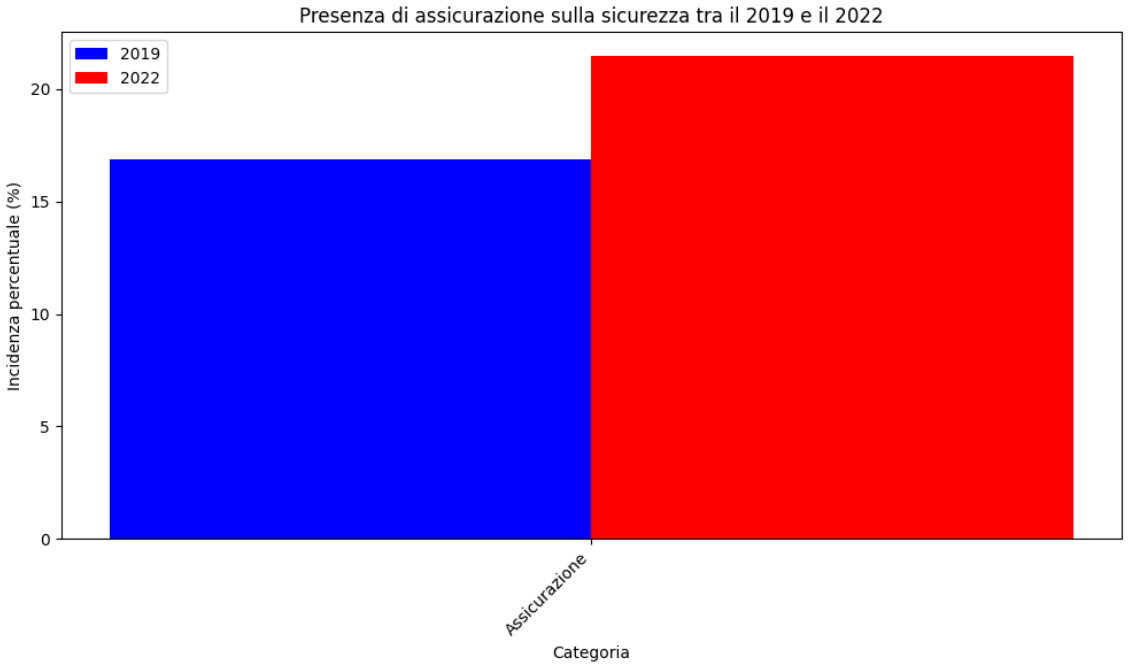

Figura 3.8: Assicurazioni contro attacchi ICT 2019 vs 2022

Dal grafico emerge chiaramente un aumento significativo nella percentuale di aziende che decidono di assicurarsi contro i rischi legati agli attacchi informatici, passando dal 16% nel 2019 al 22% nel 2022. Questo incremento può essere interpretato come un segnale del crescente riconoscimento da parte delle imprese del rischio informatico. Con l'aumentare della complessità delle minacce, molte aziende preferiscono affidarsi a coperture assicurative per mitigare i potenziali impatti finanziari legati agli attacchi.

3.4.4 Incremento delle misure di sicurezza

Oltre alla tendenza verso l'esternalizzazione del rischio tramite l'adozione di assicurazioni, le aziende italiane hanno anche adottato progressivamente diverse misure di sicurezza preventive per ridurre l'incidenza degli attacchi informatici. L'analisi aggregata degli indicatori tra il 2019 e il 2022 mostra un generale incremento delle misure di sicurezza adottate dalle imprese.

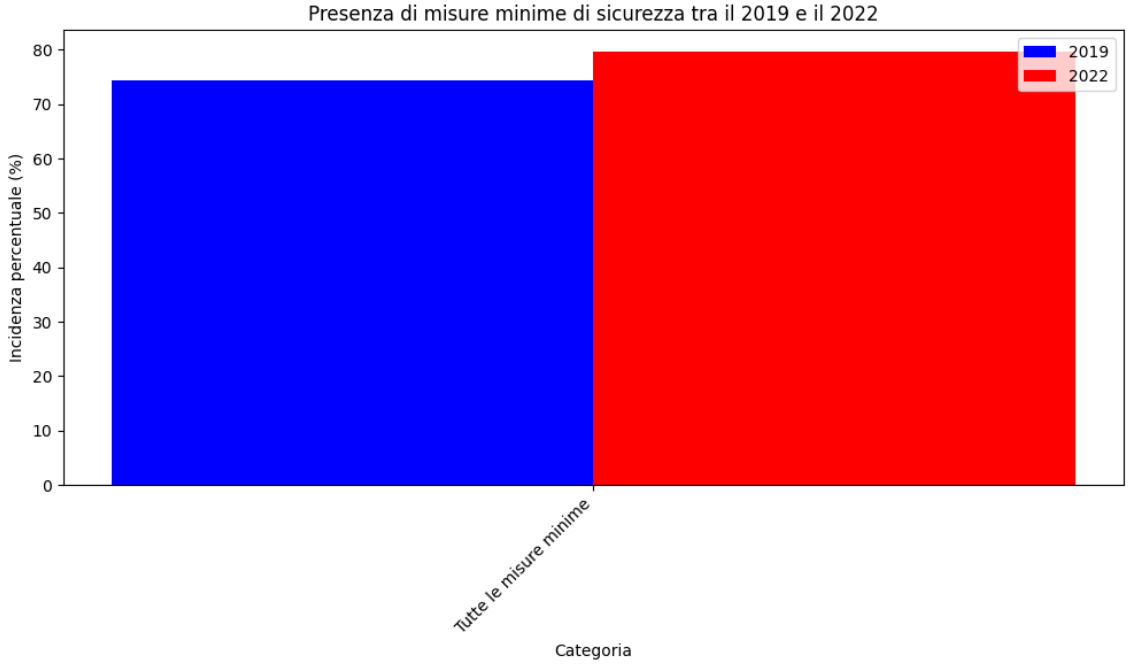

Figura 3.9: Misure minime di sicurezza 2019 vs 2022

Come possiamo osservare dal grafico, l'adozione delle misure di sicurezza minime è aumentata sensibilmente, passando dal 70% al 75%. Questo dimostra che, nonostante la crescente complessità delle minacce, le imprese italiane stanno reagendo adottando misure di sicurezza più complete per proteggere le proprie infrastrutture ICT.

Il secondo grafico fornisce un'analisi più dettagliata di quali misure di sicurezza sono state maggiormente adottate nel periodo 2019-2022.

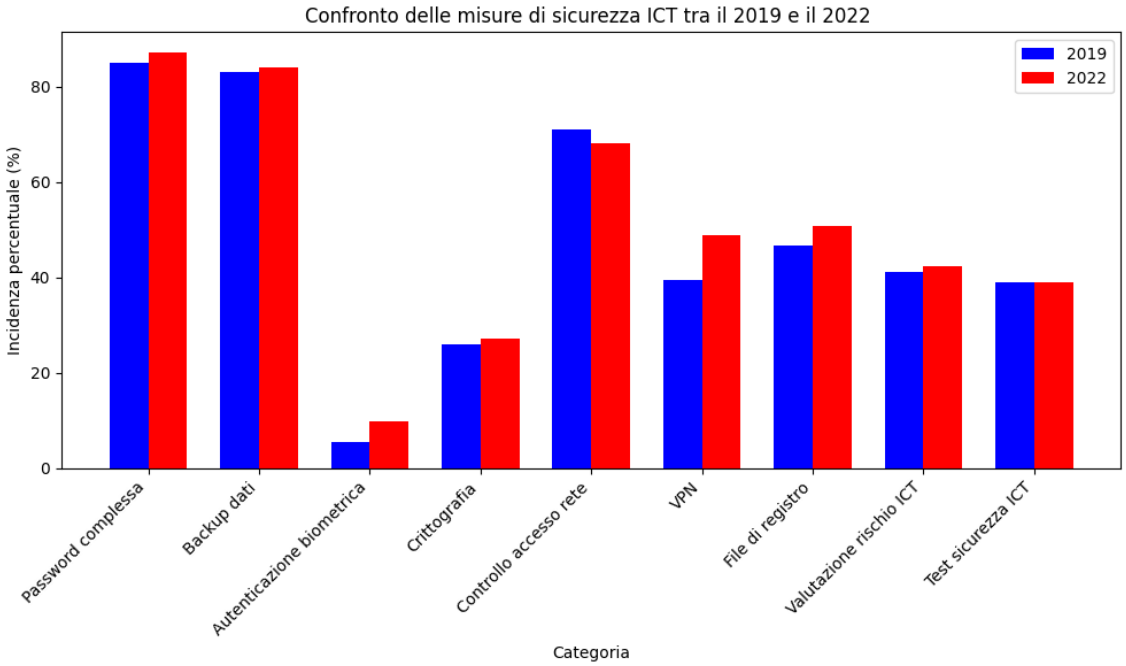

Figura 3.10: Incremento delle singole misure di sicurezza 2019 vs 2022

Da quest'analisi più specifica emerge che le misure come l'adozione di VPN aziendali, il backup dei dati, e l'autenticazione biometrica hanno registrato gli incrementi più significativi. L'adozione delle VPN, in particolare, risulta essere la misura con il maggiore incremento, riflettendo la diffusione del lavoro da remoto e la necessità di garantire l'accesso sicuro alle reti aziendali da postazioni esterne.

L'autenticazione biometrica e la crittografia sono altre misure che mostrano un aumento costante, a indicare che le aziende stanno investendo in tecnologie di sicurezza avanzate per prevenire accessi non autorizzati e proteggere i dati sensibili.

In generale, quasi tutte le misure di sicurezza mostrate nel grafico hanno visto un aumento nell'adozione tra il 2019 e il 2022, ad eccezione del controllo di accesso alla rete, che ha registrato un leggero calo. Questo potrebbe essere dovuto al fatto che alcune aziende preferiscono soluzioni come la crittografia o le VPN per gestire l'accesso ai dati aziendali in modo sicuro e remoto.

Questa evoluzione delle misure di sicurezza suggerisce una maggiore consapevolezza del rischio e la volontà delle aziende di investire in soluzioni più sofisticate per prevenire gli attacchi informatici.

3.4.5 Efficacia delle misure di sicurezza

Dopo aver esaminato l'incremento delle misure di sicurezza adottate dalle aziende, è fondamentale valutare l'efficacia di questi interventi in termini di riduzione degli attacchi informatici. Utilizzando i dati relativi agli investimenti in sicurezza ICT e l'incremento degli attacchi tra il 2019 e il 2022, è stato possibile costruire un'analisi comparativa.

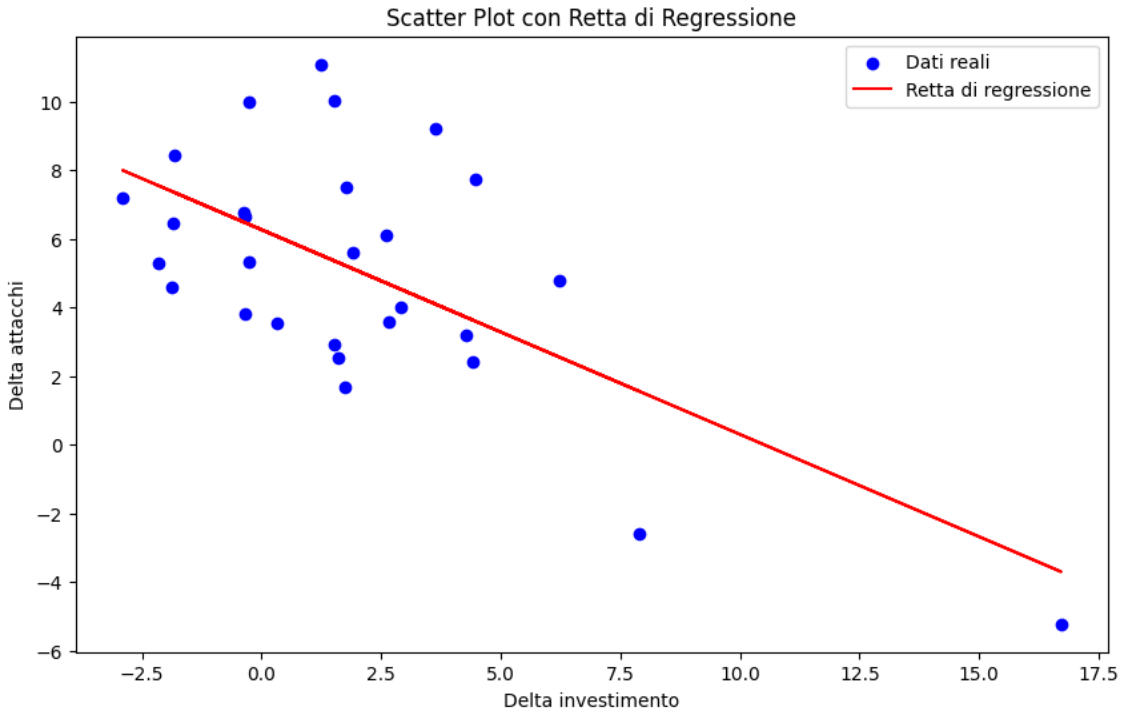

Figura 3.11: Confronto tra investimenti in sicurezza e variazione degli attacchi 2019 vs 2022

Dal grafico si può osservare una relazione inversa tra l'incremento degli investimenti in sicurezza ICT e la variazione degli attacchi subiti: i settori che hanno investito maggiormente in misure di sicurezza hanno registrato un aumento più contenuto degli attacchi rispetto a quelli che hanno investito meno. La retta di regressione evidenzia questa tendenza in modo statisticamente significativo, con un p-value di 0.0002.

Questo suggerisce che gli investimenti in misure di sicurezza hanno avuto un impatto positivo nel limitare l'aumento degli attacchi, nonostante la complessità crescente delle minacce informatiche.

3.5 Comparazione dimensionale delle imprese

Nell'analisi aggregata delle imprese italiane, abbiamo osservato trend generali riguardanti la cybersecurity, come l'andamento degli attacchi e la risposta in termini di misure di sicurezza adottate. Tuttavia, le dimensioni aziendali giocano un ruolo cruciale nella gestione e nell'esposizione al rischio informatico. Le imprese di maggiori dimensioni tendono a essere bersagli più appetibili per i cybercriminali, a causa della loro visibilità e della complessità dei sistemi che gestiscono, così come delle risorse più ampie a disposizione per la protezione.

In questa sezione, analizzeremo come la dimensione dell'azienda influisce sulla probabilità di subire attacchi e sugli investimenti in sicurezza, confrontando i risultati tra micro, piccole, medie e grandi imprese. L'obiettivo è capire se le imprese di maggiori dimensioni siano effettivamente più soggette agli attacchi e se adottino maggiori misure di sicurezza rispetto a quelle di dimensioni minori, mettendo in relazione questi risultati con l'analisi precedente delle imprese aggregate.

Come accennato, per le imprese suddivise per dimensioni, il dataset non offre lo stesso livello di dettaglio disponibile per i singoli settori. I dati disponibili riguardano i seguenti settori:

- Fornitura di energia
- Totale servizi non finanziari
- Totale attività economiche
- Costruzioni
- Attività manifatturiere

3.5.1 Confronto dell'incidenza degli attacchi informatici per dimensione aziendale

Il primo confronto che possiamo fare riguarda l'incidenza degli attacchi informatici in base alla dimensione aziendale. Osservando il grafico seguente, emergono tendenze significative.

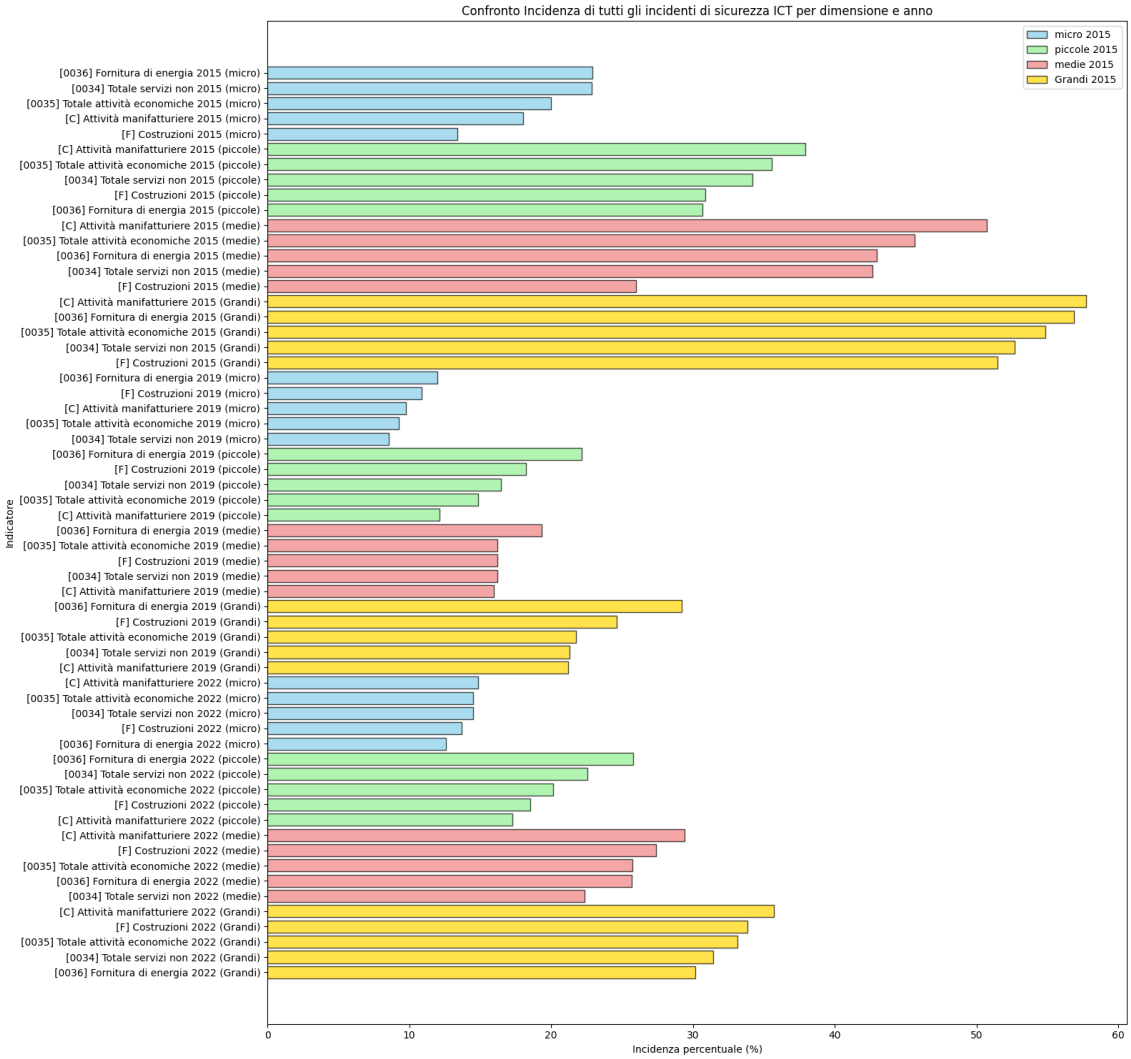

Figura 3.12: Confronto incidenza degli attacchi informatici tra le dimensioni delle imprese

In generale, i dati mostrano una tendenza simile a quella osservata per le imprese aggregate: un calo degli attacchi dal 2015 al 2019, seguito da un leggero aumento nel 2022. Tuttavia, emergono alcune differenze fondamentali:

- **Grandi imprese**: Le aziende di maggiori dimensioni sono costantemente le più colpite. Ciò è coerente con l'idea che queste imprese siano obiettivi più attraenti per i cybercriminali, sia per la loro visibilità sia per la quantità di dati sensibili che gestiscono. Questo trend è in linea con l'analisi aggregata

delle imprese, ma il livello di attacchi per le grandi aziende è decisamente più elevato rispetto alla media complessiva.

- **Micro e piccole imprese**: Presentano un'incidenza di attacchi più bassa, in linea con il fatto che queste aziende rappresentano obiettivi meno appetibili per i cybercriminali. Questo rispecchia il trend generale osservato nell'analisi aggregata, ma l'incidenza degli attacchi è significativamente inferiore rispetto alle grandi imprese.

3.5.2 Confronto sulla consapevolezza e preparazione dei dipendenti

Un altro aspetto chiave dell'analisi riguarda la consapevolezza e la preparazione dei dipendenti in materia di cybersecurity. Il grafico seguente evidenzia una differenziazione significativa tra le imprese di diverse dimensioni:

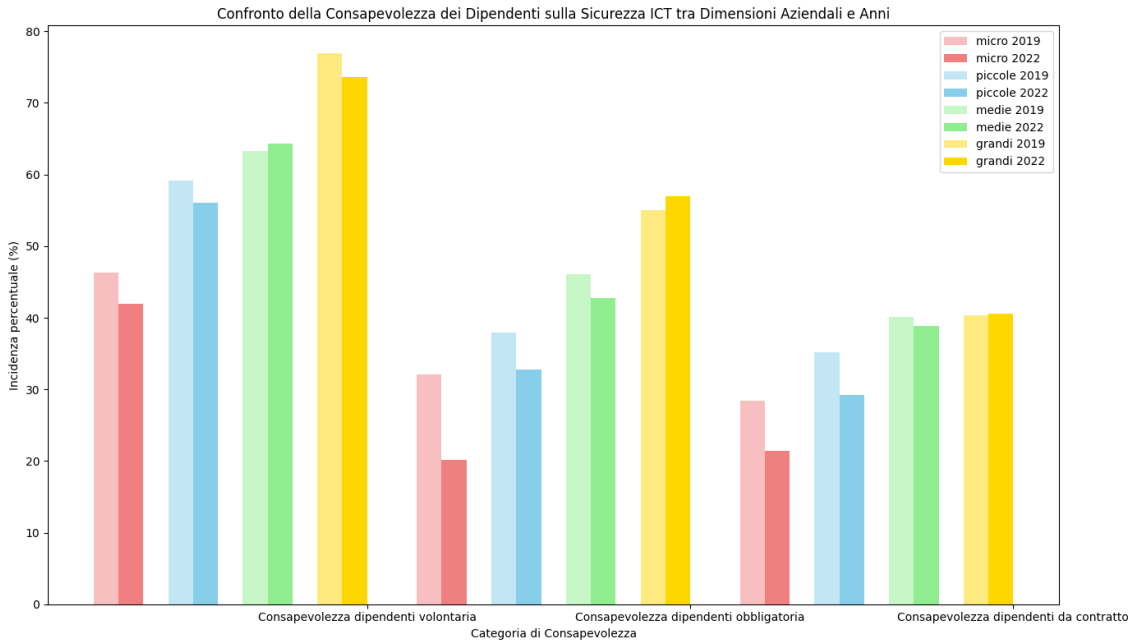

Figura 3.13: Confronto consapevolezza tra aziende di tutte le dimensioni

In questo caso, le differenze rispetto all'analisi aggregata sono notevoli:

- **Grandi imprese**: A differenza del trend generale, le grandi imprese hanno aumentato la consapevolezza obbligatoria e contrattuale dal 2019 al 2022, a indicare un approccio più strutturato e organizzato nella gestione della sicurezza. Questo si spiega con il fatto che le grandi aziende hanno maggiori risorse per implementare programmi di formazione e preparazione interna, e l'aumento della consapevolezza riflette la crescente attenzione verso la cybersecurity.
- **Micro, piccole e medie imprese**: Queste aziende hanno visto una riduzione della consapevolezza interna nello stesso periodo. Ciò può essere attribuito a una minore capacità di investimento in programmi di formazione, oppure a una crescente tendenza a esternalizzare le funzioni di sicurezza, riducendo l'attenzione interna.

In generale, questo conferma che le grandi aziende adottano un approccio più proattivo e strutturato rispetto alle piccole e medie imprese, il che è coerente con il loro ruolo come obiettivi più interessanti per i cybercriminali.

3.5.3 Confronto delle misure di sicurezza adottate

Per quanto riguarda le misure di sicurezza, le grandi imprese mostrano una maggiore adozione di tecnologie avanzate rispetto alle piccole e medie imprese, come possiamo vedere dal grafico seguente:

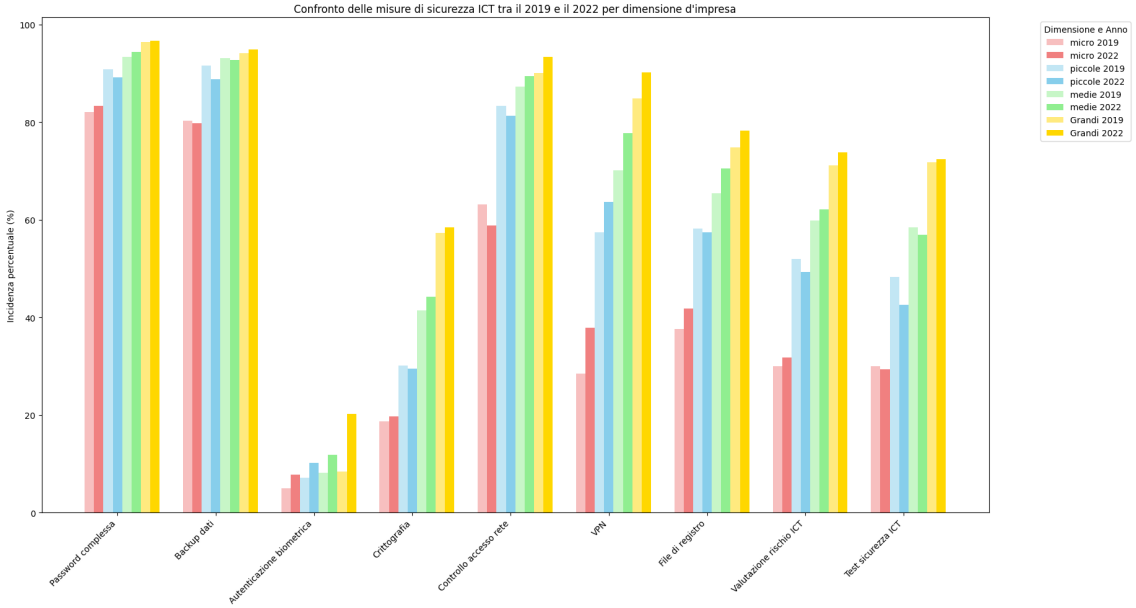

Figura 3.14: Confronto misure di sicurezza tra le dimensioni delle imprese

- **Grandi imprese**: Le grandi aziende sono le uniche ad aver aumentato l'adozione di tutte le misure di sicurezza analizzate, con particolare enfasi su autenticazione biometrica e VPN aziendali. Questo evidenzia una maggiore preparazione e reattività, confermando che, grazie a risorse economiche più ampie, queste imprese possono investire in misure di sicurezza più complesse e avanzate. La loro capacità di adottare un'ampia gamma di soluzioni di difesa dimostra un approccio più strutturato alla cybersecurity, coerente con la loro maggiore esposizione agli attacchi.

- **Piccole e medie imprese**: Queste aziende mostrano tendenze positive, ma in modo meno uniforme rispetto alle grandi imprese. L'adozione di misure più avanzate, come i test di sicurezza, è meno comune, mentre soluzioni di base come backup dei dati e password complesse rimangono tra le pratiche più diffuse. Questo riflette una tendenza tipica delle piccole e medie imprese, che tendono a concentrarsi su misure di sicurezza essenziali, ma faticano a investire in soluzioni più sofisticate a causa di risorse limitate o priorità diverse.

Infine, il grafico seguente mostra il confronto del delta di adozione delle misure minime di sicurezza per le diverse dimensioni aziendali:

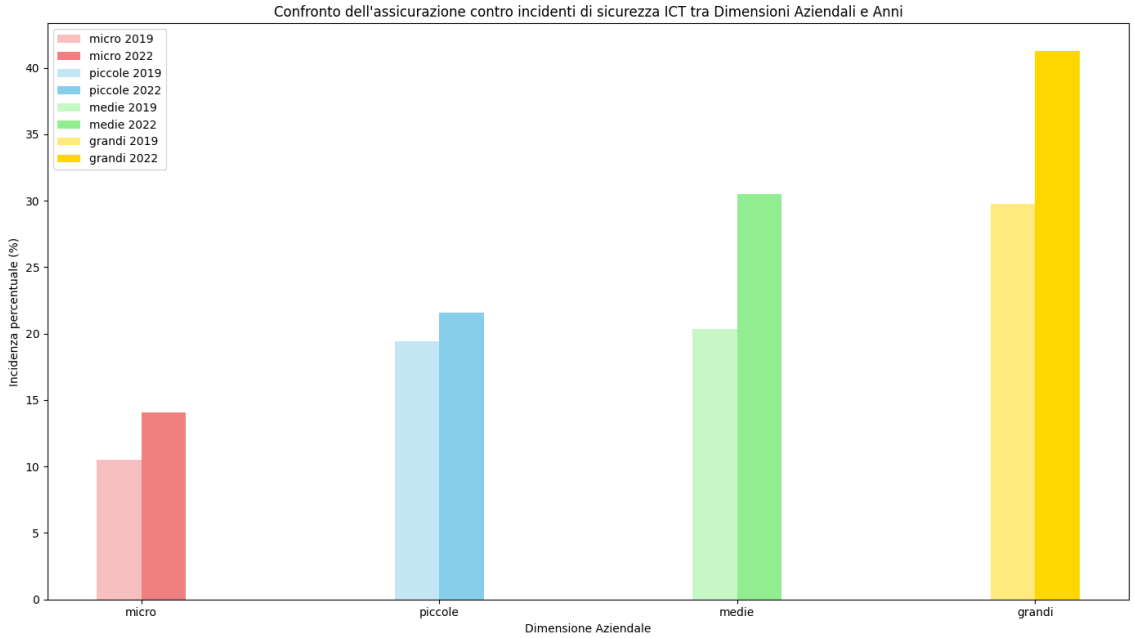

Figura 3.15: Confronto del delta di adozione delle misure minime di sicurezza per dimensione aziendale

Osservando il grafico, si nota come il delta maggiore nell'adozione delle misure minime di sicurezza sia registrato tra le grandi imprese. Questo conferma la loro maggiore capacità di adottare misure di sicurezza su più fronti, coerente con i risultati precedenti che evidenziano come queste aziende, grazie a risorse e strutture più avanzate, siano in grado di implementare una gamma più completa di strumenti di sicurezza.

3.5.4 Conclusioni sulla comparazione dimensionale

In sintesi, la dimensione aziendale influisce notevolmente sia sulla probabilità di subire attacchi informatici sia sulla risposta in termini di misure di sicurezza. Le grandi imprese, essendo bersagli più appetibili e con risorse maggiori, adottano misure di sicurezza più avanzate e hanno una consapevolezza interna più elevata rispetto alle piccole e medie imprese. Questo è in linea con quanto osservato nell'analisi aggregata, ma conferma che le grandi imprese tendono a essere più reattive e strutturate nella loro gestione della cybersecurity.

3.6 Confronto dati reali in base alla classificazione della letteratura

In questa sezione finale ci concentreremo sull'analisi degli indicatori principali visti in precedenza, confrontando i diversi settori sulla base della classificazione derivata dalla letteratura. Il riferimento principale per la nostra analisi è la Figura 3.1.

Osservando la figura, si nota immediatamente come la distribuzione dei punti non riempia tutto il grafico, ma si disponga quasi lungo una linea retta che parte dall'origine verso il terzo quadrante. Questo rende difficile classificare i settori in quattro categorie mantenendo un numero omogeneo di settori per ciascun cluster. In particolare, risulta complesso identificare e classificare settori appartenenti al secondo quadrante, che rappresenta un'alta interdipendenza di mercato ma una bassa interdipendenza tecnica.

Inizialmente, costruiremo quattro cluster utilizzando i settori più rappresentativi. La suddivisione considerata è la seguente:

Bassa interdipendenza di mercato e bassa interdipendenza tecnica

- **Industrie tessili, abbigliamento, costruzioni:** Sebbene questi settori possano utilizzare strumenti digitali, non si basano generalmente su network software condivisi, il che giustifica la loro classificazione in questo cluster.

- **Costruzioni:** Settore che non ha una forte interdipendenza tecnica. Utilizza software specifici per la gestione dei progetti, ma non dipende molto da network software condivisi. Il mercato delle costruzioni è relativamente stabile, influenzato più da investimenti a lungo termine che da dinamiche di domanda rapide.

Bassa interdipendenza tecnica, alta interdipendenza di mercato

- **Industrie alimentari:** Le aziende di questo settore tendono a utilizzare meno infrastrutture software condivise.

Alta interdipendenza tecnica, bassa interdipendenza di mercato

- **Attività professionali, scientifiche e tecniche:** Settore che utilizza spesso software specializzato e network condivisi, come piattaforme di ricerca e strumenti di collaborazione.

- **Trasporto e magazzinaggio:** Le reti logistiche condivise e i sistemi software per la gestione delle flotte, monitoraggio e magazzino giustificano l'inclusione di questo settore in questo cluster.

Alta interdipendenza tecnica e alta interdipendenza di mercato

- **Telecomunicazioni:** Questo settoro fa largo uso di network e infrastrutture software condivise, come i servizi cloud e le piattaforme di gestione dei contenuti (CMS). Inoltre, è influenzato da dinamiche di mercato rapide e in costante evoluzione.

- **Alloggio:** L'utilizzo di piattaforme globali di prenotazione come Booking o Airbnb giustifica il suo posizionamento in questo cluster, vista l'elevata interdipendenza tecnica e la dinamicità del mercato.

3.6.1 Confronto degli indicatori tra i cluster

Calcolando la media per ciascun cluster per gli indicatori considerati, confronteremo adesso i valori di alcuni parametri chiave. L'aspettativa è quella di osservare, specialmente in relazione agli investimenti in sicurezza, una minore propensione a investire da parte del cluster con alta interdipendenza tecnica e bassa interdipendenza di mercato rispetto al suo opposto. Come suggerito dalla letteratura, le aziende che appartengono al primo cluster potrebbero essere disincentivate a investire in sicurezza a causa del fenomeno del free riding, mentre quelle nel secondo cluster dovrebbero investire di più a causa dei fallimenti di mercato legati alle esternalità di mercato.

3.6.2 Analisi degli attacchi

Cominciamo analizzando il numero di attacchi subiti dai vari cluster.

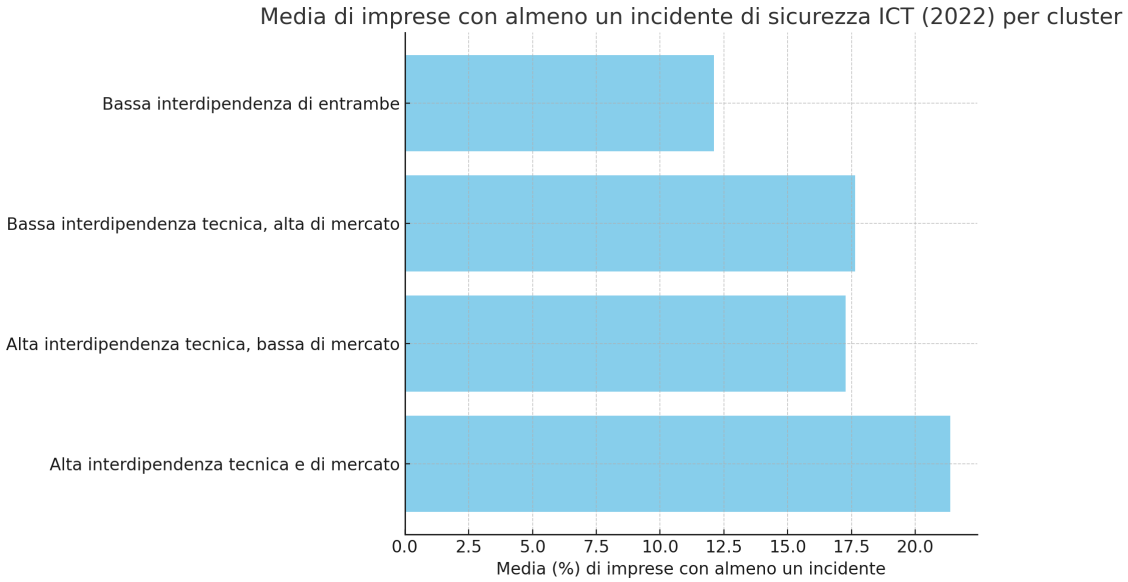

Figura 3.16: Media delle imprese con almeno un incidente di sicurezza ICT (2022) per cluster

Dalla figura emerge che il cluster con alta interdipendenza sia tecnica che di mercato è il più colpito dagli attacchi informatici. Seguono i cluster con un solo tipo di interdipendenza elevato (tecnica o di mercato), che mostrano valori simili. Infine, il cluster con bassa interdipendenza in entrambe le dimensioni è quello con il numero di attacchi più basso.

3.6.3 Correlazione tra interdipendenza e attacchi

Analizzando i dati, si nota che la correlazione tra interdipendenza e numero di attacchi sembra essere più legata a un fattore di digitalizzazione generale piuttosto che al concetto teorico di interdipendenza tecnica o di mercato. In altre parole, non è l'interdipendenza in sé a causare un aumento degli attacchi, ma piuttosto il fatto che gli indicatori utilizzati riflettono anche il livello di digitalizzazione delle imprese.

Le aziende più digitalizzate sono naturalmente più esposte agli attacchi informatici, semplicemente perché hanno un maggiore utilizzo di tecnologie e infrastrutture digitali.

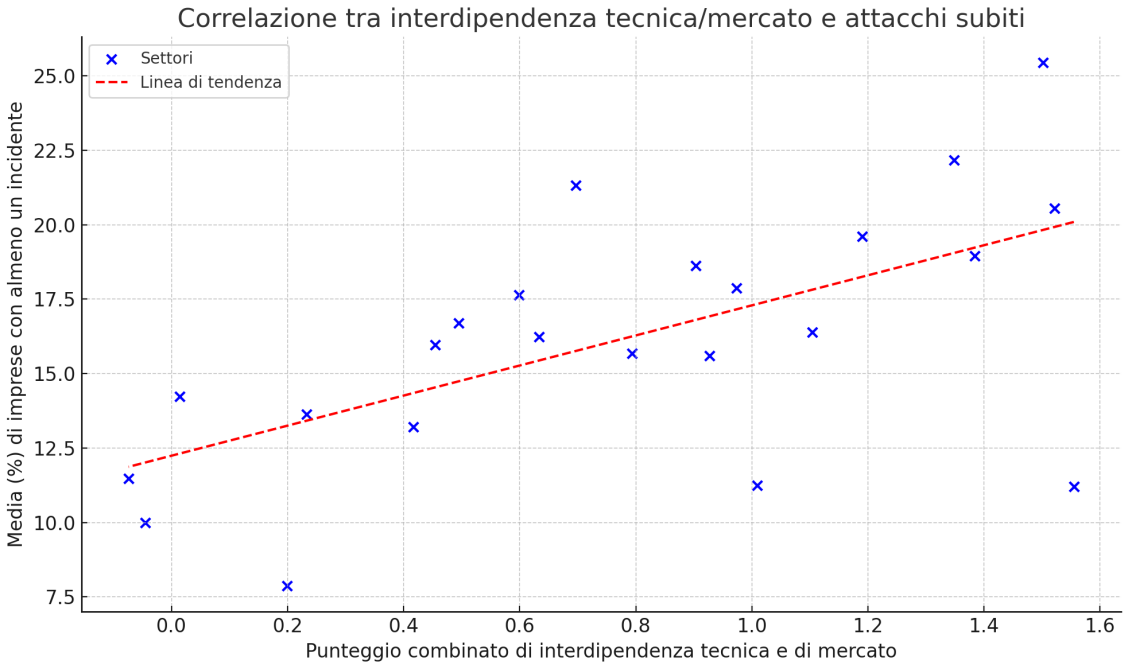

Figura 3.17: Correlazione tra interdipendenza tecnica/mercato e attacchi subiti

Questo grafico mostra che, indipendentemente dalla combinazione di interdipendenza tecnica o di mercato, all'aumentare della digitalizzazione (rappresentata dall'indicatore combinato), aumenta anche il numero di attacchi. In pratica, è la maggiore esposizione digitale a rendere queste imprese più vulnerabili agli attacchi, piuttosto che la presenza o meno di interdipendenze specifiche.

3.6.4 Analisi delle misure di sicurezza

Quanto appena osservato può essere ulteriormente verificato analizzando il livello medio di misure di sicurezza adottate dai diversi cluster.

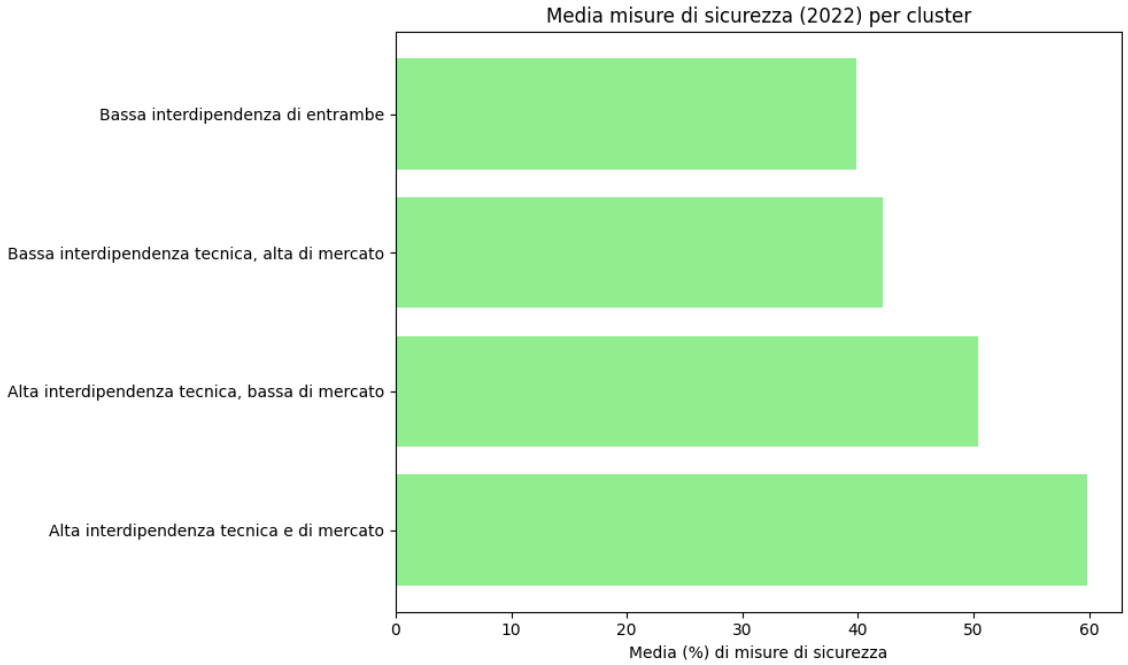

Figura 3.18: Media delle misure di sicurezza adottate per cluster

Dal grafico emerge che il cluster con alta interdipendenza tecnica e di mercato adotta il maggior numero di misure di sicurezza, seguito dai cluster con alta interdipendenza tecnica e di mercato separatamente. Anche in questo caso, il cluster con bassa interdipendenza sia tecnica che di mercato adotta meno misure di sicurezza.

Questo risultato è in linea con l'idea che dove ci sono più attacchi, si adottano più misure di sicurezza per difendersi.

Per ottenere delle indicazioni rilevanti per la letteratura, è utile analizzare i livelli di investimento in sicurezza. Come menzionato in precedenza, non disponiamo di dati diretti sulle spese o sugli investimenti specifici in cybersicurezza per ogni azienda. Tuttavia, possiamo utilizzare il delta delle misure di sicurezza adottate da un anno all'altro come proxy per stimare gli investimenti.

L'idea è che, se in un settore si osserva un aumento significativo delle misure di sicurezza da un anno all'altro, è ragionevole assumere che siano stati effettuati investimenti in quella direzione. Pertanto, confrontando il delta di sicurezza tra i cluster, possiamo ipotizzare che i cluster con il maggiore incremento nelle misure di sicurezza siano anche quelli che hanno investito di più.

Questo approccio presenta chiaramente dei limiti: sebbene possiamo osservare il cambiamento nel numero di misure adottate, non abbiamo informazioni sul costo specifico dell'implementazione di ciascuna misura. Tuttavia, rappresenta comunque

un buon punto di partenza per una prima analisi degli investimenti in sicurezza nei diversi settori.

Investimenti in misure di sicurezza: analisi dei delta

Per ottenere una visione più dettagliata degli investimenti in sicurezza, possiamo utilizzare il delta delle misure di sicurezza adottate tra il 2019 e il 2022 come proxy per stimare gli investimenti. Sebbene non disponiamo di dati diretti sugli investimenti finanziari, l'analisi del cambiamento nelle misure adottate ci offre una stima ragionevole degli investimenti effettuati.

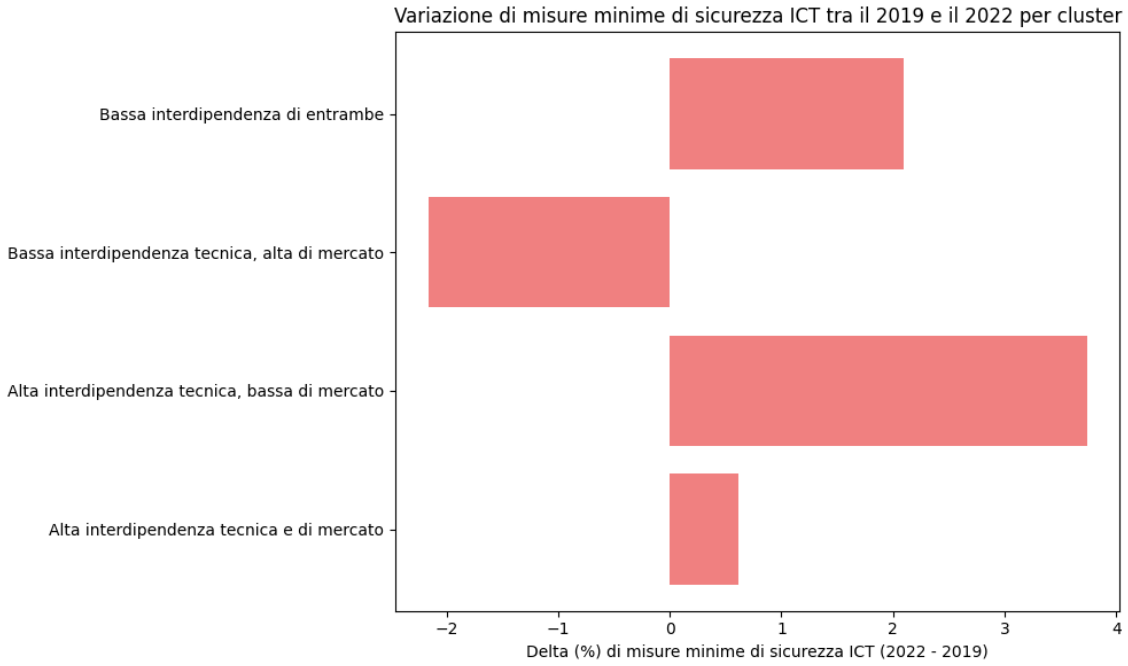

Figura 3.19: Delta delle misure di sicurezza adottate per cluster (2019-2022)

Osservando il grafico, emerge una situazione incoerente. I delta di sicurezza tra il 2019 e il 2022 non mostrano una crescita uniforme tra i cluster. Anzi, alcuni settori, come quello con bassa interdipendenza tecnica e alta di mercato, registrano persino un delta negativo, suggerendo una riduzione delle misure di sicurezza adottate. Questo potrebbe riflettere un contesto in cui alcune imprese si sono trovate ad affrontare difficoltà economiche o hanno considerato sufficienti le misure già in atto.

Per comprendere meglio i delta tra i cluster, si è deciso di creare due nuovi raggruppamenti: da un lato, i settori con interdipendenza di mercato superiore a quella tecnica, e dall'altro, i settori con interdipendenza tecnica superiore a quella di mercato. Questo ci permette di confrontare direttamente come le imprese con diverse interdipendenze abbiano modificato il loro approccio alla sicurezza.

Cluster con interdipendenza di mercato superiore a quella tecnica:

0033 Settore ICT

26 Fabbricazione di computer e prodotti elettronici

47 Commercio al dettaglio

53 Servizi postali e attività di corriere

55 Alloggio

61 Telecomunicazioni

79 Agenzie di viaggio e tour operator

C Attività manifatturiere

Cluster con interdipendenza tecnica superiore a quella di mercato:

0031 Attività professionali, scientifiche e tecniche

0036 Fornitura di energia elettrica e gas

0049 Trasporto e magazzinaggio

F Costruzioni

JC Informatica ed altri servizi

Il grafico seguente riporta i risultati di questa analisi:

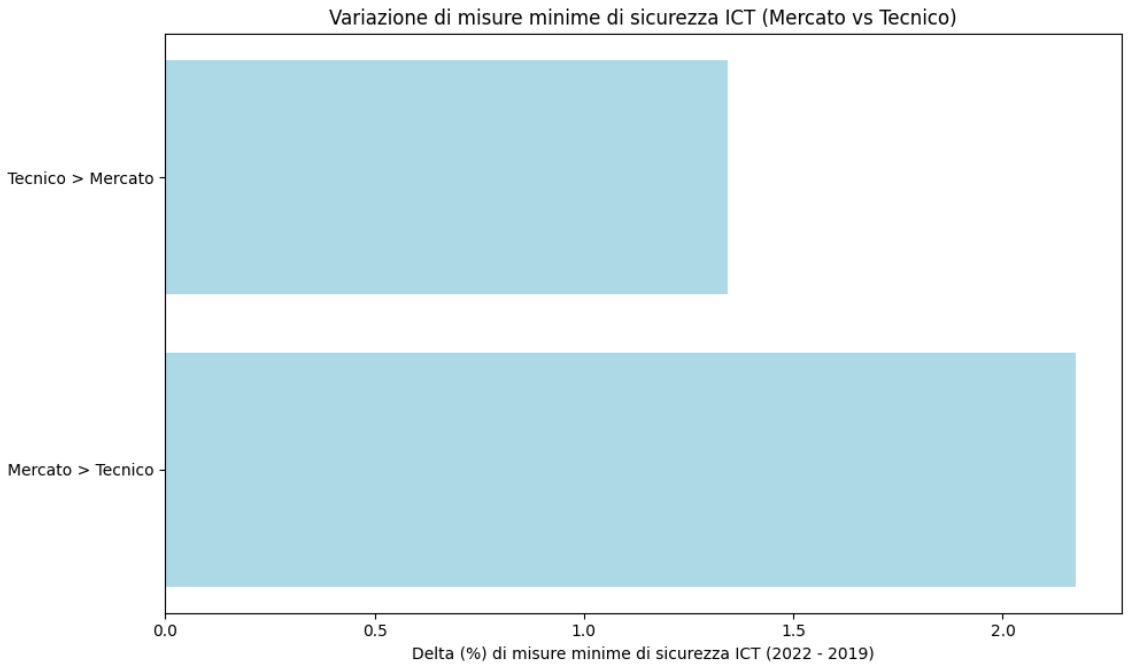

Figura 3.20: Confronto delle misure di sicurezza adottate per cluster con interdipendenza tecnica superiore vs. interdipendenza di mercato superiore

Da questo confronto emerge chiaramente che i settori con interdipendenza di mercato superiore a quella tecnica hanno investito di più nelle misure di sicurezza rispetto

ai settori con interdipendenza tecnica superiore. Questo risultato può essere interpretato come una conferma della tendenza a sottoinvestire in sicurezza nei settori caratterizzati da interdipendenza tecnica, coerente con la teoria del *free riding*. Al contrario, i settori con elevata interdipendenza di mercato tendono a investire di più per mitigare i rischi legati alla crescente esposizione a dinamiche di mercato in rapida evoluzione.

3.7 Conclusioni

In sintesi, questa analisi evidenzia che i settori con alta interdipendenza tecnica e di mercato sono i più vulnerabili agli attacchi informatici e adottano più misure di sicurezza per proteggersi. Tuttavia, l'investimento in sicurezza è meno pronunciato nei settori caratterizzati da interdipendenza tecnica, suggerendo un possibile problema di sottoinvestimento. Questi risultati aprono la strada a futuri studi più dettagliati che potranno esplorare ulteriormente questa tendenza, utilizzando dati più completi e specifici sugli investimenti in cybersicurezza.

4 Conclusioni

La digitalizzazione avvenuta negli ultimi decenni rappresenta una delle più grandi rivoluzioni dei nostri tempi, trasformando il modo di vivere, lavorare e comunicare per individui, imprese e governi. Per le imprese, in particolare, ha comportato un aumento significativo dell'efficienza e della produttività, grazie alla possibilità di automatizzare molti processi e di prendere decisioni migliori basate sull'analisi dei dati dei clienti.

Tuttavia, accanto ai numerosi benefici, le nuove tecnologie hanno portato anche nuove sfide inaspettate. La stessa capacità tecnologica che ci permette di scambiare informazioni con facilità offre ai malintenzionati la possibilità di sottrarle, mettendo a rischio i dati personali e aziendali. I sistemi digitali che semplificano il lavoro possono, infatti, esporci a gravi conseguenze in caso di manomissione o indisponibilità.

Di conseguenza, parallelamente alla crescita della digitalizzazione, è aumentata anche l'importanza della cybersicurezza. Questa disciplina è diventata fondamentale per proteggere le nuove tecnologie da usi impropri, divulgazioni non autorizzate e manomissioni esterne. In Italia, solo nel 2023, gli investimenti in cybersicurezza hanno superato i 2 miliardi di euro, come riportato nel documento ufficiale del Clusit, rendendo questo ambito uno dei settori di investimento più rilevanti e meritevoli di attenzione.

Come ogni investimento, anche la cybersicurezza non è esente da fallimenti di mercato, definiti come situazioni in cui gli investimenti non riflettono i costi e benefici reali per la società. È quindi importante studiarne le cause e gli effetti per migliorare la regolamentazione e ottimizzare la spesa. In questa tesi si è cercato di raccogliere la letteratura esistente sugli investimenti in cybersicurezza e di classificarla in relazione ai diversi fallimenti di mercato. Si è osservato come, in presenza di interdipendenze tecniche — ovvero la partecipazione di diverse aziende a un'unica rete informatica — si manifesti un problema di sottoinvestimento dovuto al fenomeno del free riding, in cui alcuni attori traggono beneficio da un bene o servizio senza contribuire al costo della sua fornitura. In questo contesto, gli individui o le aziende possono essere incentivati a non investire in sicurezza, confidando che altri si faranno carico dei costi, portando così a una sottofornitura del bene rispetto al livello ottimale. Allo stesso tempo, è emerso che le interdipendenze di mercato, ovvero la possibilità di "rubare" clienti in caso di attacco a un concorrente, portano le imprese a investire in modo eccessivo per proteggere la propria base di utenti e acquisirne di nuovi.

Successivamente, sono stati analizzati i dati dell'ISTAT relativi alla digitalizzazione e alla cybersicurezza in Italia, con l'obiettivo di verificare se i risultati empirici riscontrati sul territorio italiano fossero in linea con quanto emerso dalla letteratura. Prima di tutto, i vari settori sono stati classificati secondo il codice ATECO nelle diverse aree di fallimento di mercato (interdipendenze tecniche o interdipendenze di mercato), creando dei cluster di settori con caratteristiche simili, utilizzando alcuni degli indicatori come proxy. I dati generali relativi alla cybersicurezza sono stati poi esaminati per tutti i settori, evidenziando tendenze significative, come l'aumento degli attacchi tra il 2019 e il 2022, complice il trasferimento forzato verso il digitale di molte funzioni aziendali a causa della pandemia di COVID-19. È stata inoltre rilevata una crescente tendenza delle imprese a esternalizzare la gestione della sicurezza, sia affidandosi ad aziende specializzate sia sottoscrivendo assicurazioni specifiche.

Un confronto tra imprese di diverse dimensioni ha confermato la tendenza delle aziende più grandi a essere maggiormente attaccate e, di conseguenza, a incrementare le proprie misure di sicurezza.

Infine, utilizzando i delta tra le misure di sicurezza adottate dalle imprese come proxy del loro livello di investimento, si è analizzato se i settori con una maggiore interdipendenza di mercato investano effettivamente più delle imprese con prevalenza di interdipendenza tecnica. I risultati di questa analisi hanno confermato quanto previsto dalla letteratura scientifica, anche per il contesto italiano: i settori caratterizzati da una prevalenza di interdipendenza tecnica presentano un tasso di investimento in cybersicurezza inferiore rispetto a quelli con una maggiore interdipendenza di mercato. Questo suggerisce che le imprese con interdipendenza di mercato siano più motivate a proteggere la propria base di clienti, mentre quelle con interdipendenza tecnica tendano a fare affidamento sugli investimenti altrui, contribuendo a un problema di sottoinvestimento complessivo.

Una volta identificata l'effettiva presenza di fallimenti di mercato, è fondamentale proporre delle misure di regolamentazione per ridurre tali inefficienze. Per quanto riguarda il sottoinvestimento delle imprese caratterizzate da alta interdipendenza tecnica, l'Unione Europea ha stilato diverse proposte per mitigare gli effetti del free riding. In particolare, il Digital Operational Resilience Act (DORA) introduce misure specifiche per responsabilizzare tutti i partecipanti a infrastrutture digitali condivise e imporre misure minime di sicurezza. DORA assegna la responsabilità della resilienza operativa a ogni partecipante, inclusi i fornitori terzi di servizi critici, riducendo così il rischio di free riding e garantendo che ciascun attore contribuisca attivamente alla sicurezza del sistema. Inoltre, DORA stabilisce requisiti minimi di sicurezza obbligatori per tutte le aziende, contribuendo a una maggiore protezione collettiva e alla riduzione delle vulnerabilità legate alle infrastrutture condivise.

Osservando poi il Piano Nazionale di Ripresa e Resilienza (PNRR), emerge un'attenzione significativa alla digitalizzazione delle piccole e medie imprese (PMI), riconoscendone il ruolo cruciale nell'economia italiana. Il PNRR prevede incentivi per l'adozione di tecnologie avanzate come il cloud computing e l'intelligenza artificiale, nonché fondi per progetti di innovazione e formazione delle competenze digitali.

Tuttavia, i dati analizzati in questa tesi mostrano come le PMI investano meno in cybersicurezza rispetto alle grandi aziende e tendano a esternalizzare maggiormente la gestione della sicurezza, rendendole più vulnerabili al fenomeno del free riding.

Per il futuro, sarebbe auspicabile creare un fondo specifico per lo sviluppo di misure di cybersicurezza nelle PMI, al fine di incentivare l'investimento diretto in sicurezza e ridurre la dipendenza dagli investimenti degli altri attori del network. Considerando l'attuale disponibilità limitata di fondi pubblici, questo fondo potrebbe essere alimentato attraverso risorse provenienti da iniziative come Industria 4.0 e successivi piani di sviluppo tecnologico. In questo modo, si garantirebbe una maggiore resilienza dell'intero sistema economico e si mitigherebbe il rischio di vulnerabilità collettive causate dalla dipendenza dagli investimenti di pochi soggetti.

In definitiva, la digitalizzazione offre un potenziale enorme, ma richiede un approccio strategico e coordinato per garantire la sicurezza e la sostenibilità di questi sviluppi. Solo attraverso politiche mirate e un impegno collettivo sarà possibile sfruttare appieno i benefici della trasformazione digitale, riducendo al contempo i rischi che essa comporta. La cybersicurezza non deve essere vista come un costo, ma come un investimento essenziale per garantire la resilienza del nostro sistema economico e sociale, promuovendo un futuro digitale più sicuro e prospero per tutti.

Ringraziamenti

Voglio esprimere la mia sincera gratitudine a tutti coloro che hanno contribuito al successo di questo progetto. Ringrazio il Prof. Carlo Cambini per la sua guida indispensabile. Un grazie particolare ai miei genitori per il loro amore e supporto costante. Un ringraziamento speciale a Camilla, per essere stata al mio fianco durante tutto il percorso. Infine, un grazie agli amici per il loro incoraggiamento e supporto.

5 Referenze

Cybersecurity 360. https://www.cybersecurity360.it/outlook/ma-quanto-ci-costano-i-data-breach-facciamo-un-po-di-conti/ https://www.cybersecurity360.it

Rapporto clusit 2022. https://www.saccani.net/wp-content/uploads/2022/03/Rapporto-Clusit-marzo-2022$_{bw}eb.pdf$

Relazione per la cybersecurity nazionale. https://www.acn.gov.it/portale/relazione-annuale-2022

Report IBM 2023. https://www.ibm.com/reports/data-breach

Dati Istat. http://dati.istat.it/Index.aspx?QueryId=24860

DORA https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora

Fedele e Roner (2021). https://onlinelibrary.wiley.com/doi/10.1111/joes.12456

Alexandre de Corniere and Greg Taylor (2021). https://www.tse-fr.eu/sites/default/files/TSE/docun

Wing Man Wynne Lam, Jacob Seifert (2023). https://onlinelibrary.wiley.com/doi/10.1111/joie.12316

Noé Ciet and Marianne Verdier (2022). https://papers.ssrn.com/sol3/papers.cfm?abstract$_id = 4304898$

Accenture. (2020). Innovate for Cyber Resilience. https://www.accenture.com/$_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf$

Acemoglu, D., Malekian, A., Ozdaglar, A. (2016). Network security and contagion. Journal of Economic Theory, 166, 536–585.

Amir, E., Levi, S., Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. Review of Accounting Studies, 23(3), 1177–1206.

Anderson, R., Moore, T. (2006). The economics of information security. Science, 314(5799), 610–613.

Anderson, R. J. (2001). Why information security is hard – an economic perspective. In Proceedings of the 17th Annual Computer Security Applications Conference (pp. 358–365).

Arce, D. G. (2018). Malware and market share. Journal of Cybersecurity, 4(1), 1–6.

Arce, D. G. (2020). Cybersecurity and platform competition in the cloud. Computers Security, 93, 101774.

Arce, D. G., Sandler, T. (2005). Counterterrorism: A game-theoretic analysis. The Journal of Conflict Resolution, 49(2), 183–200.

Baryshnikov, Y. (2012). IT security investment and Gordon-Loeb's 1/e rule. Proceedings of the Workshop on the Economics of Information Security (WEIS).

BEREC - Body of European Regulators for Electronic Communications. (2018). Report on infrastruc- ture sharing. https://berec.europa.eu/eng/document$_register/subject_matter/bere$
$berec - report - on - infrastructure - sharing.$

Biancotti, C., Cristadoro, R. (2018). The machine stops: The price of cyber (in)security. https://voxeu.org/article/ price-cyber-insecurity.

Biancotti, C., Cristadoro, R., Di Giuliomaria, S., Fazio, A., Partipilo, G. (2017). Cyber attacks: An economic policy challenge. https://voxeu.org/article/cyber-attacks-economic-policy-challenge.

Böhme, R. (2012). Security audits revisited. International Conference on Financial Cryptography and Data Security, 129–147.

Böhme, R. (2016). Back to the roots: Information sharing economics and what we can learn for security. Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, 1–2.

Böhme, R., Schwartz, G. (2010). Modeling cyber-insurance: Towards a unifying framework. Proceedings of the Workshop on the Economics of Information Security (WEIS).

Cavusoglu, H., Raghunathan, S., Yue, W. T. (2008). Decision-theoretic and game-theoretic approaches to IT secu- rity investment. Journal of Management Information Systems, 25(2), 281–304.

Center for Strategic International Studies-McAfee. (2018). The Economic Impact of Cybercrime: No Slowing Down. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact- cybercrime.pdf .

Cerdeiro, D. A., Dziubiński, M., Goyal, S. (2017). Individual security, contagion, and network design. Journal of Economic Theory, 170, 182–226.

Chawla, S., Niu, F. (2009). The price of anarchy in Bertrand games. Proceedings of the 2009 ACM Conference on Electronic Commerce, 305–314.

Cisco. (2020). Consumer Privacy Survey - Protecting Data Privacy to Maintain Digital Trust. https: //www.cisco.com/c/dam/en$_us/about/doing_business/trust -$
$center/docs/cybersecurity - series - 2020 - cps.pdf?CCID = cc$000742.

Comino, S., Manenti, F. M. (2014). Industrial organization of high-technology markets: The internet and informa- tion technology. Edward Elgar publishing.

Dinkova, M., El-Dardiry, R., Overvest, B. (2020). Cyber incidents, security measures and financial returns: Empir- ical evidence from Dutch firms. Discussion Paper CPB Netherlands Bureau for Economic Policy Analysis, (411).

Dziubiński, M., Goyal, S. (2013). Network design and defence. Games and Economic Behavior, 79, 30–43.

Dziubiński, M., Goyal, S. (2017). How do you defend a network? Theoretical Economics, 12(1), 331–376.

Florêncio, D., Herley, C. (2013). Where do all the attacks go? Economics of Information Security and Privacy III, 13–33.

Gal-Or, E., Ghose, A. (2005). The economic incentives for sharing security information. Information Systems Research, 16(2), 186–208.

Gao, X., Zhong, W. (2016). Economic incentives in security information sharing: the effects of market structures. Information Technology and Management, 17(4), 361–377.

Garcia, A., Horowitz, B. (2007). The potential for underinvestment in internet security: Implications for regula- tory policy. Journal of Regulatory Economics, 31(1), 37–55.

Garcia, A., Sun, Y., Shen, J. (2014). Dynamic platform competition with malicious users. Dynamic Games and Applications, 4(3), 290–308.

Geer, D., Jardine, E., Leverett, E. (2020). On market concentration and cybersecurity risk. Journal of Cyber Policy, 5(1), 9–29.

Gordon, L. A., Loeb, M. P. (2002). The economics of information security investment. ACM (Association for Computing Machinery) Transactions on Information and System Security, 5(4), 438–457.

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

Gordon, L. A., Loeb, M. P., Lucyshyn, W. (2003b). Sharing information on computer systems security: An eco- nomic analysis. Journal of Accounting and Public Policy, 22(6), 461–485.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., Zhou, L. (2015a). Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb model. Journal of Information Security, 06(01), 24–30.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., Zhou, L. (2015b). Increasing cybersecurity investments in private sector firms. Journal of Cybersecurity, 1(1), 3–17.

Goyal, S., Vigier, A. (2014). Attack, defence, and contagion in networks. The Review of Economic Studies, 81(4), 1518–1542.

Grossklags, J., Christin, N., Chuang, J. (2008). Secure or insure? A game-theoretic analysis of information security games. Proceedings of the 17th International Conference on World Wide Web, 209–2018.

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(5), 338–349.

Heal, G., Kunreuther, H. (2005). IDS models of airline security. The Journal of Conflict Resolution, 49(2), 201–217.

Hirshleifer, J. (1983). From weakest-link to best-shot: The voluntary provision of public goods. Public Choice, 41(3), 371–386.

Huang, D. C., Hu, Q., Behara, R. S. (2008). An economic analysis of the optimal information security investment in the case of a risk-averse firm. International Journal of Production Economics, 114, 793–804.

IBM Corporation. (2020). Cost of a Data Breach Report. https://www.ibm.com/security/digital-assets/cost-data- breach- report//pdf .

Iqbal, A., Guo, M., Gunn, L., Babar, M. A., Abbott, D. (2019). Game theoretical modelling of network/cyber security. IEEE Access, 7, 154167–154179.

Janakiraman, R., Lim, J. H., Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. Journal of Marketing, 82, 85–105.

Jeong, C. Y., Lee, S.-Y. T., Lim, J.-H. (2019). Information security breaches and IT security investments: Impacts on competitors. Information Management, 56, 681–695.

Jiang, L., Anantharam, V., Walrand, J. (2011). How bad are selfish investments in network security? IEEE/ACM Transactions on Networking, 19(2), 549–560.

Jianqiang, G., Shue, M., Weijun, Z. (2015). Analyzing information security investment in networked supply chains. 2015 International Conference on Logistics, Informatics and Service Sciences (LISS), 1–5.

Jo, A.-M. (2017). The effect of competition intensity on software security - An empirical analysis of security patch release on the web browser market. Proceedings of the 16th Annual Workshop on the Economics of Information Security (WEIS 2017).

Kamhoua, C. A., Kwiat, L., Kwiat, K. A., Park, J. S., Zhao, M., Rodriguez, M. (2014). Game theoretic modeling of security and interdependency in a public cloud. Proceedings of the 2014 IEEE 7th International Conference on Cloud Computing, 514–521.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics, (In press).

Kopp, E., Kaffenberger, L., Wilson, C. (2017). Cyber Risk, Market Failures, and Financial Stability. IMF Working Papers, 17(185), 1.

Koutsoupias, E., Papadimitriou, C. (2009). Worst-case equilibria. Computer Science Review, 3, 65–69.

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, https://doi.org/10.1111/risa.13713.

Kunreuther, H., Heal, G. (2003). Interdependent security. Journal of Risk and Uncertainty, 26(2-3), 231–249. Laszka, A., Felegyhazi, M., Buttyán, L. (2014). A survey of interdependent security games. ACM Computing Sur- veys, 47(2), 23:1–23:38.

Lattanzio, G., Ma, Y. (2020). Corporate innovation in the cyber age. SSRN Electronic Journal.

Lelarge, M. (2009). Economics of malware: Epidemic risks model, network externalities and incentives. 47th Annual Allerton Conference on Communication, Control, and Computing, 1353–1360.

Lelarge, M. (2012). Coordination in network security games: A monotone comparative statics approach. IEEE Jour- nal on Selected Areas in Communications, 30(11), 2210–2219. Lelarge, M., Bolot, J. (2008). Network externalities and the deployment of security features and protocols in the internet. ACM SIGMETRICS Prformance Evaluation Review, 36(1), 37–48. Liang, X., Xiao, Y. (2013). Game theory for network security. IEEE Communications Surveys Tutorials, 15(1), 472–486. Liao, C.-H., Chen, C.-W. (2014). Network externality and incentive to invest in network security. Economic Mod- elling, 36, 398–404.

Liu, X., Qian, X., Pei, J., Pardalos, P. M. (2018). Security investment and information sharing in the market of complementary firms: Impact of complementarity degree and industry size. Journal of Global Optimization, 70(2), 413–436.

Manshaei, M. H., Zhu, Q., Alpcan, T., Bacşar, T., Hubaux, J.-P. (2013). Game theory meets network security and privacy. ACM Computing Surveys, 45(3), 1–39.

Merrick, K., Hardhienata, M., Shafi, K., Hu, J. (2016). A survey of game theoretic approaches to modelling decision-making in information warfare scenarios. Future Internet, 8(3), 34.

Microsoft Corporation. (2016). Microsoft Advanced Threat Analytics Datasheet 2016. https://download.microsoft. com/download/C/F/6/CF62335F-C46B-4D84-B0C9-363A89B0C5E6/Microsoft$_a dvanced_t hreat_a nalytics_d atasheet.pdf$.

Miura-Ko, A. R., Yolken, B., Bambos, N., Mitchell, J. (2008). Security investment games of interdependent orga- nizations. 46th Annual Allerton Conference on Communication, Control, and Computing, 252–260.

Nagurney, A., Nagurney, L. S. (2015). A game theory model of cybersecurity investments with information asym- metry. Netnomics, 16(1-2), 127–148.

National Research Council. (2014). At the nexus of cybersecurity and public policy: Some basic concepts and issues. Washington DC: The National Academies Press.

Nguyen, K. C., Alpcan, T., Basar, T. (2009). Stochastic games for security in networks with interdependent nodes. 2009 International Conference on Game Theory for Networks, 679–703.

O'Donnell, A. J. (2008). When malware attacks (anything but Windows). IEEE Security Privacy, 6(3), 68–70. Paulsen, C. (2016). Cybersecuring small businesses. Computer, 49(8), 92–97.

Ponemon Institute. (2019). 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses. https://www. keepersecurity.com/en$_G$B/*ponemon*2019.*html*.

Qian, X., Pei, J., Liu, X., Zhou, M., Pardalos, P. M. (2019). Information security decisions for two firms in a market with different types of customers. Journal of Combinatorial Optimization, 38(4), 1263–1285.

Riek, M., Böhme, R. (2016). Estimating the costs of consumer-facing cybercrime: A tailored instrument and representative data for six EU countries. Workshop on the Economics of Information Security (WEIS).

Riordan, M. H. (2014). Security in partnerships. Mimeo, Department of Economics, Columbia University.

Rochet, J.-C., Tirole, J. (2003). Platform competition in two-sided markets. Journal of the European Economic Association, 1(4), 990–1029.

Roner, C., Di Caterina, C., Ferrari, D. (2021). Exponential tilting for zero-inflated interval regression with appli- cations to cybersecurity survey data. Mimeo, Faculty of Economics and Management, Free University of Bozen- Bolzano.

Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., Wu, Q. (2010). A survey of game theory as applied to network security. Proceedings of the 43rd Hawaii International Conference on System Sciences, 1–10.

Rue, R., Pfleeger, S. L. (2009). Making the best use of cybersecurity economic models. IEEE Security Privacy Magazine, 7(4), 52–60.

Sales, N. A. (2013). Regulating cyber security. Northwestern University Law Review, 107(4), 1503–1568.

Sen, R., Verma, A., Heim, G. R. (2020). Impact of cyberattacks by malicious hackers on the competition in soft- ware markets. Journal of Management Information Systems, 37(1), 191–216.

Tanaka, H., Matsuura, K., Sudoh, O. (2005). Vulnerability and information security investment: An empirical analysis of e-local government in Japan. Journal of Accounting and Public Policy, 24(1), 37–59.

The White House. (2003). The National Strategy to Secure Cyberspace. https://us-cert.cisa.gov/sites/default/files/ publications/cyberspace$_s$*trategy.pdf*.

Tirole, J. (2017). Economics for the Common Good. Princeton University Press.

UK Government - Dept. for Digital, Culture, Media and Sport. (2020a). Cyber Security Breaches Survey 2020. https: //www.gov.uk/government/statistics/cyber-security-breaches-survey-2020.

UK Government - Huawei Cyber Security

Evaluation Centre Oversight Board. (2020b). Annual Report. https: //www.gov.uk/government/pub cyber-security-evaluation-centre-oversight-board-annual- report- 2020.

Varian, H. R. (2004). System reliability and free riding. In J. J. Camp S. Lewis (Eds.)

Wang, S. (2017). Optimal Level and Allocation of Cybersecurity Spending: Model and Formula. SSRN Electronic Journal.

Willemson, J. (2006). On the Gordon and Loeb model for information security investment. Proceedings of the Work- shop on the Economics of Information Security (WEIS).

Willemson, J. (2010). Extending the Gordon and Loeb model for information security investment. 2010 Interna- tional Conference on Availability, Reliability and Security. IEEE, 258–261.

Wolff, J., Lehr, W. (2017). Degrees of ignorance about the costs of data breaches: What policymakers can and can't do about the lack of good empirical data. SSRN Electronic Journal.

Woods, D. W., Böhme, R. (2021). Systematization of knowledge: Quantifying cyber risk. IEEE Symposium on Security Privacy.

5.1 Appendice

Espressione K. Il guadagno atteso per l'azienda i quando non subisce alcuna violazione può essere formalizzato da una distribuzione di probabilità binomiale di Poisson definita come:

$$K = \sum_{A \subseteq F_k \setminus \{i\}} \frac{X}{N} \frac{|A|}{N - |A|} \prod_{j \in A} \left(\frac{1}{I_j + 1} \right) \prod_{z \in A^c} \left(1 - \frac{1}{I_z + 1} \right)$$

dove:

- A: Insieme delle aziende che subiscono un attacco informatico.
- A^c: Insieme delle aziende che non subiscono un attacco informatico (complemento di A).
- $|A|$: Numero di aziende che subiscono un attacco informatico.
- F_k: Insieme delle $N - 1$ aziende nel mercato (escludendo l'azienda i).