POLITECNICO DI TORINO
Repository ISTITUZIONALE

The economics of cyber risk: a survey of the literature

Original
The economics of cyber risk: a survey of the literature / Abrardi, L., Comino, S., Grassini, S.. - In: ECONOMIA E POLITICA INDUSTRIALE. - ISSN 0391-2078. - (2026). [10.1007/s40812-025-00370-3]

Availability:
This version is available at: 11583/3006992 since: 2026-01-27T12:07:19Z

Publisher:
Springer Nature

Published
DOI:10.1007/s40812-025-00370-3

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

26 November 2026

Journal of Industrial and Business Economics
https://doi.org/10.1007/s40812-025-00370-3

The economics of cyber risk: a survey of the literature

Laura Abrardi[1] · **Stefano Comino**[2] · **Sasha Grassini**[1]

Received: 31 October 2024 / Revised: 4 July 2025 / Accepted: 24 July 2025
© The Author(s) 2025

Abstract
Cyber risk has emerged as a critical challenge for businesses, governments, and individuals. The greater availability of data, the increasing dependence on digital infrastructures, and the ever-advancing level of sophistication of cybercriminals have intensified both the occurrence and impact of security breaches. Literature on the economic aspects of cybersecurity originates from several distinct research areas and employs various approaches, emphasising the multifaceted nature of this phenomenon. This survey presents an overview of the economic dimension of cybersecurity, summarising the main findings of this rich and interdisciplinary literature. Our survey focuses on the four key actors involved in cybersecurity: hackers, companies, consumers/users and regulators. We provide an overview of the motivations and strategies employed by hackers, examine how companies and users protect themselves against cyber risks and respond to breaches, and analyse the economic and financial consequences. We also discuss the policy instruments available to regulators to mitigate both the likelihood and the impact of cyberattacks. In the final section, we suggest some potential directions for future research. (*JEL* D8, L86, L20)

Keywords Cyber risk · Online safety · Hackers · Data · Regulation

This study was carried out within the "Cyber Resilience: Markets, Investments and Regulation" project - funded by European Union - Next Generation EU within the PRIN 2022 PNRR program (D.D.1409 del 14/09/2022 Ministero dell'Università e della Ricerca, CUP: E53D23016530001). This manuscript reflects only the authors' views and opinions and the Ministry cannot be considered responsible for them.

This publication is part of the project PNRR-NGEU which has received funding from the MUR–DM 351/2022.

Extended author information available on the last page of the article

Published online: 19 August 2025

1 Introduction

The digital era has fundamentally reshaped the way societies function, introducing unprecedented levels of connectivity and transforming everyday activities—from banking and shopping to social interactions and access to public services. The growing dependence on digital technologies has turned online environments into prime targets for criminal activity. Cyberattacks can take many forms—such as phishing, malware injection, or distributed denial-of-service (DDoS) attacks— in the same way they target a wide range of victims, from individuals and businesses to public services and network infrastructures. Their objectives vary, as they may include data exfiltration, theft of sensitive information, ransom requests, and business disruption. Estimating the economic damages caused by cyber incidents is challenging, as they often include intangible elements such as reputational harm and a loss of trust among users or customers of the affected company. These challenges are further compounded in cases where the attacks target critical infrastructures, such as hospitals, disrupting patient care and delaying treatments, or power grids, causing widespread blackouts. While existing estimates agree that the overall cost of cyberattacks is significant, accurately assessing the full extent of these damages remains difficult. For example, Jamilov et al. (2023) estimate that the global cost of cyber risk exceeds $200 billion annually. Other projections are even more pessimistic, estimating the global cost of cybercrime at over $8 trillion in 2023 (Fleck and Richter, 2024) and at $9 trillion in 2024 (Petrosyan, 2023).

The literature on the economics of cybersecurity combines a variety of approaches. It ranges from studies that use traditional economic tools to analyse the behaviour of companies and users who invest in protecting themselves against cybercriminals, to more technical IT-related contributions. Studies also include research that focuses on managerial aspects, as well as investigations that explore the perspectives of hackers or the victims of attacks through psychological or sociological lenses. This survey aims to synthesise contributions from these diverse areas and provide an up-to-date overview of the economic dimensions of cybersecurity.

We focus on the four key actors involved in cybersecurity: hackers, firms, consumers/users, and regulators. We have examined the behaviour and characteristics of hackers across several dimensions, including their motivations, strategies, targets, and the dynamics of collaboration and competition within the hackers' community. This relatively extensive body of research reveals that hackers are a highly heterogeneous group, and viewing them as a monolithic entity is overly simplistic. Recent studies consistently find that, when targeting firms, hackers tend to focus on larger companies due to the higher potential returns and the greater number of entry points available for attack. Other factors influencing cyberattacks on firms include the industry sector to which the company belongs and the structure of its computer network.

When looking at firms and users, the literature has focused on the incentives to invest in cybersecurity and continuously update software and devices to keep them up-to-date against cyberattacks. The misalignment of incentives among the actors contributing to breach prevention drives security failures (Anderson and Moore, 2006). In their review, Fedele and Roner (2022) highlight that the economics literature is mainly concerned with the consequences of two types of externalities and

how these impact firms' incentives to invest in cybersecurity. Market and technical externalities affect investment returns, leading to greater or smaller departures from the welfare-maximising level of security. The management literature has extensively studied the incentives of vendors and users in managing system security appropriately, with a timely release and installation of patches.

The empirical literature on the consequences of cyberattacks has predominantly focused on their short-term effects, particularly examining stock price movements following the announcement of a data breach. In contrast, long-term effects are more difficult to quantify due to the presence of several potential confounding factors.

Regulators play a crucial role in addressing inefficiencies in the incentives to contribute to cybersecurity. Various policy tools—such as liability regimes, security standards, and mandatory cyber insurance—are discussed in the literature, highlighting the advantages and disadvantages of each measure.

The remainder of the paper is organised as follows. Section 2 reviews the literature on hackers, focusing on their motivations, strategies, and targets. Section 3 examines how firms and users respond to cyber threats, discussing the incentives to invest in cybersecurity and the management of cyber risks. In Sect. 4, we analyse the economic and financial consequences of cyberattacks, distinguishing between short-term and long-term effects. Section 5 is devoted to evaluating the effectiveness of various policy instruments in supporting cybersecurity. For each of these sections, we provide a synoptic table summarising the most relevant bibliographic references, their approaches, and key findings. Finally, Sect. 6 concludes the paper and outlines potential directions for future research.

2 Hackers' incentives, strategies and tools

The term hacker is frequently used generically, but the hacker landscape is highly heterogeneous in terms of motivations, ethical stances, and skill sets (Jordan and Taylor, 1998; Madarie, 2017). The European Union Agency for Cybersecurity (ENISA) classifies hackers into four groups ranging from state-sponsored groups – sometimes under the direct control of the military or the intelligence apparatus of their country – to cybercriminals – mainly motivated by financial gains—and from hackers-for-hire—providing services to other cyber groups – to hacktivists – fuelled by solid ethical motivations but endowed by much fewer resources than other groups (ENISA, 2023). Chng et al. (2022) propose a finer-grained classification, recognising how hackers' activity may be driven by curiosity, recognition by the community, revenge, espionage, ideology or financial returns. Depending on the motivations of the hackers, attacks may target private companies, public services, or take the form of cyber warfare or attempts to influence public opinion in a foreign country.

Cyberattacks can also vary widely in the techniques employed. Table 1 summarises the most common ones. These may involve the installation of malware designed to damage the victim's computer, phishing emails that deceive users into revealing credentials or clicking malicious links, and ransomware that blocks access to data or systems until a payment is made. Other strategies involve denial-of-service (DDoS)

Table 1 Types of cyberattacks

Attack Type	Description	Examples
Phishing, Social Engineering	Attack where the hacker sends fake emails or messages to steal information.	A deceptive email, apparently sent from the customer's bank, requesting bank credentials.
Malware, Ransomware	Malicious software designed to damage, hide, or steal information, threatening a ransom payment.	Viruses that either prevent access to the system or files, or data through encryption.
DDoS (Distributed Denial of Service), Botnet	Coordinated attack that overwhelms a server or network to make it inaccessible.	Remote control of infected computers to launch DDoS attacks, send spam or flood a website with fake traffic.
SQL Injection, Cross-Site Scripting (XSS)	Injection of malicious code into a database or web pages.	Inserting malicious SQL code into a login form to access sensitive data. Inserting JavaScript code into a comment page to steal session cookies.
Man-in-the-Middle (MitM)	Interception of communications between two parties to steal or alter data.	Interception of an unsecured Wi-Fi connection to steal banking credentials.
Password Attack	Attempts to steal passwords using techniques such as repeated guessing (brute force) or cracking.	Brute force attack, trying all possible combinations to guess a password.
Zero-Day Exploit, APT (Advanced Persistent Threat)	Exploitation of a vulnerability unknown to the software vendor or a prolonged attack on an organisation to steal sensitive information.	Attack against an unpatched vulnerability (e.g., the EternalBlue exploit used by WannaCry). Silent infiltration in a company system, e.g., the Sony Pictures hack.

attacks that disrupt services, or code injections that slow down the victim's website or render its services inaccessible to customers.

In what follows, we present the main findings from the literature on hackers' strategies and the factors that influence their behaviour.

2.1 Hackers' strategies

The literature generally distinguishes between two broad categories of attacks, namely indiscriminate (non-targeted) and directed (targeted) attacks (Casey, 2003; Png and Wang, 2009).

Indiscriminate attacks, such as large-scale phishing campaigns, follow a scatter-shot logic. Thousands of emails are sent randomly, hoping that a portion of recipients will click a malicious link or download an infected attachment. Victims are not pre-selected, and success depends on volume (Gao and Zhong, 2015).

In contrast, targeted attacks are more selective and sophisticated. Cybercriminals carefully choose their victims—often based on economic, political, or reputational incentives—and employ advanced techniques such as scanning for vulnerabilities, exploiting zero-day flaws, and refined social engineering. Though less frequent, targeted attacks tend to cause more severe damage (Wu et al., 2023) and require greater effort and expertise.

In practice, these two categories often overlap. Attackers may begin with indiscriminate tactics and later exploit successful attempts in more tailored, targeted stages. To capture this complexity, Kour et al. (2025) have adopted the cyber "kill chain" framework, which models the non-cooperative game between attackers and defenders from reconnaissance to exfiltration. Game-theoretic models also explore strategic interactions between attackers and defenders (Cremonini and Nizovtsev, 2009), highlighting how multi-stage attacks and collaboration among hackers can increase effectiveness (Hausken, 2008, 2015, Hausken, 2017a, b).

While reputational rivalry can be a disincentive to information sharing, recent studies have demonstrated that cooperation between hackers, particularly in targeted attacks, can enhance success by leveraging shared knowledge of vulnerabilities (Mookerjee et al., 2011). These interactions can create "hacker-side externalities", in which a successful breach enhances the attacker's capabilities for future targets or enables ripple effects (Wu et al., 2020). However, information sharing remains a strategic choice. In some contexts, it facilitates access and increases efficiency; in others, it fuels competition among attackers, potentially reducing the individual benefit (Hausken, 2015, 2017a).

2.2 Determinants of targeted attacks

The likelihood of cyber incidents depends on several factors which affect the technical vulnerability and financial attractiveness of targets. These determinants include firms' characteristics, particularly the firm's size and industry, human factors that affect the adoption of security protocols, and technical elements such as the network structure and interconnectivity of devices.

Firm size. Geer et al. (2020) suggest that firm size influences all three dimensions of cyber risk: threat (the probability of being targeted), vulnerability (the probability of a successful attack), and impact (the severity of consequences). Larger organisations handle more data, hold more intellectual property rights and other intangible assets, and operate complex IT systems, making them attractive and more exposed targets.[1]

[1] In addition to that, the scale of a system tends to increase the time-to-patch, thus delaying fixing vulnerabilities leaving more time to exploit the breach to maximise the returns per attack.

Survey evidence from Italian firms confirms this pattern. Biancotti (2017a, b) and Bencivelli and Mogardini (2024) find that one in four firms reports at least one cyber-attack over the previous five years, with the share rising from 19.5% among firms with less than 50 employees to over 30% in firms with 50 employees or more.[2] These results are consistent with related literature, which describes how small firms tend to allocate the least resources on combating cybersecurity threats (Aldasoro et al., 2022; Junior et al., 2023). However, these figures may underestimate the true extent of attacks, especially among small firms, which may lack the tools to detect breaches or choose not to report them to avoid reputational damage.

To obtain an unbiased measure of firm-level exposure to cyber risk, Jamilov et al. (2023) apply natural language processing to data on quarterly earnings calls from 13,000 listed firms from 85 countries between 2002 and 2021, tracking mentions of cybersecurity terms to infer exposure. Their findings indicate that cyber-exposed firms tend to be larger, more liquid, and more reliant on intangible assets. Furthermore, the authors reveal that cyber risk often spills over across firms to the sectoral level.

Firm industry. Cyber threats target unevenly across sectors. Financial services, for instance, suffer up to 300 times more cyberattacks per year than other sectors (Boston Consulting Group, 2019). Healthcare and telecommunications are also frequent targets due to their handling of sensitive data or control over critical infrastructures. Biancotti, 2017a, b; Bencivelli and Mongardini, (2024) and the UK Government's Cyber Security Breaches Survey (Department for Digital, Culture, Media and Sport, 2022) confirm that financial institutions, telecoms, and tech-intensive firms are preferred targets. Firms with international operations—particularly in high-risk jurisdictions—are more vulnerable due to greater data exchange and exposure (Biancotti, 2017a, b).

Human capital may also play a role. Firms in traditional sectors or located in less industrialised regions with a lower-skilled workforce may be inadequately equipped to detect or respond to cyber threats (Biancotti, 2017a, b). The World Economic Forum (2024) highlights a widening skills gap in cybersecurity, especially across sectors with low digital maturity.

Firms operating in infrastructure networks (energy grids, oil pipelines, transportation, communications) are especially vulnerable to attacks due to the externalities inherent in networked systems. A breach in one node can cascade through the entire system (Kovenock and Roberson, 2018).

Finally, firms operating within supply chains might be subject to greater risk due to differences in cybersecurity maturity across companies (World Economic Forum, 2024). Indeed, a strong security posture by one firm can create negative externalities on the rest of the network, making weaker firms within the network more attractive targets (Bier et al., 2007; Hausken, 2008; Pym et al., 2013). This mechanism emphasises the importance of a coordinated security approach.

[2] See also Ettredge and Richardson (2003), Boasiako and Keefe (2021), Vasek et al. (2016) for evidence on the role of firm size on cyber risk.

Individuals' characteristics. While firm-level determinants are well-studied, fewer contributions focus on individual vulnerabilities. Survey and experimental studies suggest that analytical reasoning (Kelley et al., 2023), age (Sheng et al., 2010), and gender (Sheng et al., 2010; Iuga et al., 2016) may influence phishing susceptibility. Fedele et al. (2024), using administrative data on phishing attacks targeting almost 150,000 customers of an Italian bank, find that younger clients are more likely to fall victim to phishing—possibly due to greater use and trust of digital channels—but observe no significant effect from gender or place of residence.

2.3 New tools for hackers: cryptocurrencies and artificial intelligence

Technological advancements and emerging market solutions provide new tools and opportunities for illicit operations. In particular, cryptocurrencies and Artificial Intelligence (AI) have significantly influenced how attacks are conducted and monetised.

Cryptocurrencies have become a key enabler of cybercrime due to the anonymity they offer and the ability to transfer funds across borders without intermediaries. Cryptocurrencies are not only used for ransomware payments. A recent Europol (2025) report highlights how blockchain technology and cryptocurrencies are being exploited to facilitate payments and launder criminal proceeds.[3]

The role of Artificial Intelligence on cyber risk is multifaceted (ENISA, 2023). On the defensive side, AI enhances cybersecurity capabilities through improved threat detection, anomaly recognition, and real-time responses. These tools improve risk assessment and reduce security costs.[4] However, on the offensive side, AI creates new vulnerabilities by enabling sophisticated and automated cyberattacks (Mitra et al., 2024). It lowers entry barriers for attackers and increases the frequency and complexity of threats (Morgan Stanley, 2024). Adversarial attacks may also be directed towards intentionally manipulating inputs to mislead the AI model into making incorrect predictions. While AI systems can learn to detect these threats, adversaries can also use AI to observe these defensive mechanisms and develop strategies to bypass them (Truong et al., 2020)

Table 2 provides an overview of the most relevant studies discussed in this section on hackers' incentives and strategies.

Despite this, the actual impact of AI on the prevalence and intensity of cyberattacks remains debated. Khan et al. (2024) analyse global data on AI patents and cyber incidents, finding no consistent causal relationship between the diffusion of AI patents and the number of individuals affected by cyberattacks. Their findings suggest that while AI has expanded attackers' capabilities, it has so far only occasionally enabled more sophisticated threats.

[3] Foley et al. (2019) estimate that approximately $76 billion of the annual illegal activity can be linked to Bitcoin only.

[4] According to Watson and Bergman (2024) the adoption of AI-driven tools led to important efficiency gains with some firms halving breach detection and response times. Uddin et al. (2025) observe an increasing adoption of innovative generative AI practices to combat cybercrimes and related challenges. Sai et al. (2024), however, stress that developing and maintaining generative AI systems for security is extremely costly.

Table 2 Hackers' incentives and strategies

Contribution	Focus	Approach	Key Results
ENISA (2023)	Hackers' profiles and motivations	Policy/Descriptive	Hackers are classified into state-sponsored, cybercriminals, hackers-for-hire, and hacktivists.
Chng et al. (2022)	Hackers' motivations	Conceptual framework	Motivations include curiosity, recognition, revenge, ideology, espionage, and financial gain.
Casey (2003); Png and Wang (2009); Gao and Zhong (2015)	Hackers' strategies	Conceptual framework	Targeted attacks are costlier and rarer but more damaging; indiscriminate attacks are mass-scale and lower-cost.
Wu et al. (2023)	Hackers' strategies	Theoretical	Hackers exert more effort on the core asset than on the non-core asset and get higher payoffs from a targeted attack than an indiscriminate attack.
Hausken (2008, 2015, Hausken, 2017a)	Hackers' strategies	Theoretical	Multi-stage attacks and information sharing among specialised hacker groups increase effectiveness.
Hausken (2017b)	Hackers' strategies	Theoretical	Multi-stage attacks and information sharing among multiple hackers and multiple defenders increase respective effectiveness.
Biancotti (2017a, b)	Determinants of targeted attacks	Empirical (survey-based)	Larger and international firms face more attacks; underreporting is likely among smaller firms.
Bencivelli and Mongardini (2024)	Determinants of targeted attacks	Empirical (survey-based)	Nearly 90 per cent of businesses are aware of the possibility of becoming the target of a cyberattack, although this awareness does not always correspond to an adequate financial commitment to address the risks.
Jamilov et al. (2023)	Determinants of targeted attacks	Empirical	Cyber exposure correlates with size, liquidity, and sectoral spillovers.
Kovenock and Roberson (2018)	Determinants of targeted attacks	Theoretical	Highly connected systems are vulnerable due to cascading failures.
Fedele et al. (2024)	Determinants of targeted attacks	Empirical	Younger clients of banks are more likely to be phished; no gender/place-of-residence effect.
ENISA (2023)	New tools for hackers	Policy/Descriptive	Multifaceted role of AI: enhances defensive possibilities but enables sophisticated attacks.

3 Prevention of cyberattacks

Empirical evidence on firms' attitudes toward cyber risk remains limited. Bencivelli and Mongardini (2024), drawing on Bank of Italy survey data, show that nearly 90% of companies acknowledge the risk of cyberattacks. However, this awareness rarely translates into adequate financial investment. According to Biancotti (2017b), the median amount spent on cybersecurity is merely €4,530, roughly 15% of a typical worker's annual gross wages, with notable variance across sectors and firm sizes. Gordon et al. (2018), using data from a large-scale survey of senior executives in U.S.

private firms, also find widespread underinvestment, attributing it to the difficulty of quantifying returns and a prevalent "wait-and-see" attitude. Notably, firms that have already experienced a cyberattack are more likely to invest in prevention (Biancotti, 2017b).

Among defensive measures, anti-malware software is nearly ubiquitous, and almost two-thirds of firms offer cybersecurity training to employees. However, more advanced practices, such as vulnerability analysis and data encryption, are less common (Biancotti, 2017b).

On the theoretical side, Gordon and Loeb (2002) model cybersecurity investment by a monopolistic firm as a trade-off between system vulnerability and potential loss. An influential contribution by Anderson and Moore (2006) emphasises that market failures—particularly misaligned incentives and externalities—are a major source of underinvestment. Because firms in interdependent networks do not internalise the benefits of their security for others, free-riding emerges (Kunreuther and Heal, 2003; Varian, 2004). At the same time, negative externalities can also arise as investment in cybersecurity serves to redirect attacks to competitors, leading to over-investment (Acemoglu et al., 2016). Information asymmetries between firms and consumers further distort incentives, especially in competitive environments where security quality is not observable (Nagurney and Nagurney, 2015).

These failures are especially pronounced in high-tech sectors, where constant innovation introduces new vulnerabilities.[5] As a result, cybersecurity requires ongoing vigilance, patching, and adaptation. Security practices within companies are also influenced by organisational routines and culture, as suggested by the evolutionary theory of the firm (Nelson and Winter, 1985). Importantly, users play a critical role in maintaining security. However, bounded rationality—stemming from cognitive limitations and behavioural biases—often leads to delays in installing patches or neglecting security updates (Acquisti et al., 2018).

Against this backdrop, the following sections explore the main factors identified in the literature that drive efforts to prevent cyberattacks. Table 3 summarizes the most relevant results.

3.1 Externalities

Following Fedele and Roner (2022), we distinguish between two sources of externalities that influence cybersecurity investment: those stemming from technological interdependencies and those arising from market interactions.

The technical channel. Technical spillovers arise when firms are linked through shared network infrastructures. Kunreuther and Heal (2003) and Varian (2004) show that such setups often lead to free-riding and underinvestment by non-competing firms. Coordination failures further exacerbate this problem. Yet another source of

[5] An alternative point of view is presented in Arora et al. (2006). Interestingly, these authors suggest that it might be profitable for a software producer to release a 'buggy' product. The firm trades-off an early release of a 'buggy' software and the investment needed to fix it at later stages. Huang et al. (2024) argue that the release of buggy software products may also be caused by the tendency of software markets to reward first movers that release new functionalities early, hence the mantra "we'll ship it on Tuesday and get it right by version 3".

Table 3 Prevention of cyberattacks

Contribution	Focus	Approach	Key Results
Gordon and Loeb (2002)	Cybersecurity investment	Theoretical	In a monopolistic environment, there is a trade-off between the vulnerability of information and the potential losses
Anderson and Moore (2006)	Cybersecurity investment	Theoretical	Free-riding and lack of liability lead to systemic underinvestment; the need for policy intervention
Fedele and Roner (2022)	Cybersecurity investment	Literature review	Literature review on theoretical articles on the incentives to invest in cybersecurity. Importance of externalities (technical and market-related).
Kunreuther and Heal (2003)	Cybersecurity investment	Theoretical	When the magnitude of risk depends on the action of interdependent agents, either everyone invests in protection, or no one does; insurance and regulation can improve overall security
Varian (2004)	Cybersecurity investment	Theoretical	Security decisions may involve free-riding; shared-loss models lead to better security outcomes than independent loss models; coordination is crucial
Acemoglu et al. (2016)	Cybersecurity investment	Theoretical	Even well-secured agents can be vulnerable due to others' inaction with large-scale risks; central interventions (e.g. standards) can reduce systemic risk
Dziubiński and Goyal (2013)	Cybersecurity investment	Theoretical	Sparse networks often emerge as an equilibrium; targeted defence on central nodes is more efficient
Cerdeiro et al. (2017)	Cybersecurity investment	Theoretical	Densely connected networks increase contagion risk; individuals underinvest in security due to externalities; optimal design trades off efficiency vs. security
De Cornière and Taylor (2024	Cybersecurity investment	Theoretical	Investment incentives depend on the business model (price vs. ad-based)
Acquisti et al. (2018)	Users' patching incentives	Literature review	Bounded rationality causes delays in installing patches or neglecting security updates
Cavusoglu et al. (2008)	Vulnerability disclosure and patching	Theoretical	Firms tend to delay patching to reduce cost, increasing systemic risk; synchronised patching mechanisms improve global security outcomes
Choi et al. (2010)	Vulnerability disclosure and patching	Theoretical	Voluntary disclosure depends on externalities and competition; some firms benefit from hiding vulnerabilities
August and Tunca (2006)	Users' patching incentives	Theoretical	Rebate-based policies outperform mandatory or tax-based policies for patch adoption.

underinvestment by firms operating in interconnected networks: in a framework with a strategic attacker, Dziubiński and Goyal (2017) show that firms invest enough if others do the same. However, Grossklags et al. (2008) highlight that firms may opt for self-insurance instead of proactive security measures, which can be socially efficient under perfect information.

The structure of the network itself also matters. Dziubiński and Goyal (2013) show that firms may have the incentive to design dense and homogeneous networks when defence is costly. However, these are also more vulnerable to contagion, as indicated by Goyal and Vigier (2014), who advocate for star-shaped networks with centralised defence. The tension between connectivity and exposure to external threats is also the focus of Cerdeiro et al. (2017), who show that this trade-off may lead to over-investment or under-investment in security. They also find that social welfare can

be maximised in sparsely connected networks when under-investment pressures are present and in fragmented networks when over-investment pressures prevail.

Comino et al. (2025) argue that technical externalities may also arise as a consequence of regulatory obligations requiring interoperability. As services become increasingly interconnected via standardised protocols, breaches in one system may quickly propagate to others. The study compares private versus social incentives to invest in security under such regulatory conditions.

The competition channel. In competitive markets, cybersecurity investments may also produce market-based externalities. Acemoglu et al. (2016) reveal that firms may overinvest in security with the strategic intent to redirect attacks towards less-protected rivals, justifying public coordination efforts (Bandyopadhyay et al., 2014). Information asymmetries can instead reduce incentives to invest: when consumers only perceive average cybersecurity quality, the incentive to differentiate through investment declines as competition increases (Nagurney and Nagurney, 2015).

Qian et al. (2019) distinguish between loyal consumers, who never switch providers regardless of security levels, and rational consumers, who are security-concerned and may switch. The presence of loyal consumers reduces the incentives for firms to compete and invest. Liu et al. (2018) examine competition in complementary goods markets, where a cyberattack on one firm can reduce demand for the entire ecosystem. In such cases, one firm's investment benefits its competitors.

Several studies focus on the complex interplay between market power and cybersecurity investments. While large firms are a bigger target for cyberattacks (Geer et al., 2020), they may also gain a competitive advantage by attracting security-conscious customers (Gao and Zhong, 2016; Arce, 2018). Arce (2018) and Vasek et al. (2016) link platforms' market share to cybersecurity investment, challenging Anderson's (2001) view that monopolies lack incentives to invest in cybersecurity. Arce argues that market structure and cybersecurity are mutually reinforcing.

The endogenous effect of security investment on market structure and firms' business model is also the focus of De Cornière and Taylor (2024), who show that security intensifies price competition; hence, it is always underprovided in equilibrium. In ad-based models, by contrast, security increases differentiation, resulting in over-investment. These findings suggest that policy interventions (e.g. liability rules) should be tailored to the firm's market context and business model.

3.2 Identification of vulnerabilities and patching

Software and hardware vendors increasingly prioritise protecting their products, but the ever-evolving cyber threat landscape poses significant challenges. Many organisations may lack the internal expertise or resources to manage these risks effectively.

In response to the growing demand for breach prevention, the market has developed mechanisms such as vulnerability reward and bug bounty programmes, which incentivise ethical hackers to responsibly disclose security flaws (Algarni and Malaiya, 2014; Bhushan et al., 2022; Ransbotham et al., 2012). Atefi et al. (2023), using data from Chromium and Firefox vulnerability-reward programmes, document

the growing use of employing ethical hackers and structured platforms to conduct these audits.[6][7]

The literature on bug bounty programmes is expanding. Zhao et al. (2015) and Walsh and Simpson (2020) focus on the rationale for remunerating hackers. Using data from 35 bug bounty programmes, Maillart et al. (2017) show that newly launched initiatives tend to attract more hackers, as older ones quickly become saturated and yield fewer discoveries, despite higher average rewards for bugs found at later stages.

Vulnerability disclosure and the timing of patching. Initially, "security through obscurity" was a standard, keeping vulnerabilities secret to prevent their exploitation. However, research by Cremonini and Nizovtsev (2006, 2009) shows that transparent firms may deter attacks by signalling high security, thereby shifting hacker attention to weaker targets.

Choi et al. (2010) investigate the incentives of a software vendor to disclose a vulnerability and simultaneously release a patch. While disclosure improves the utility of users who install patches, it also favours "reverse engineering" by hackers, increasing the risk for those who delay the update. Hence, mandatory disclosure is not always welfare-enhancing. Canann (2019) develops a game-theoretic model suggesting that immediate disclosure is optimal only when zero-day vulnerabilities can be effortlessly discovered. When vulnerabilities are harder to detect, delaying disclosure until more users patch can reduce overall harm.

Foerderer and Schuetz (2022), analysing U.S. breach announcements from 2008 to 2018, find that firms often choose the timing of disclosures strategically—e.g., on busy news days—to reduce market reaction and mitigate reputational or financial damage.

Timing remains critical when vulnerabilities are discovered by a third party, e.g., by a user. Immediate public disclosure increases awareness and pressures vendors to act quickly, but delayed disclosure—after a patch is ready—better protects users.[8] Arora et al. (2008) model this dynamic, showing that a social planner may need to shorten the non-disclosure window to accelerate patching. Cavusoglu et al. (2008) highlight that synchronisation between patch release and user updates is socially

[6] The authors collect vulnerability reports from September 2, 2008, to September 13, 2022. For each report, the Chromium issue tracker provides a list of affected components, impacted release channels, and comments that include conversations among internal stakeholders.

[7] Examples of bug bounty platforms are HackerOne (trusted by companies like PayPal, Nintendo, AT&T, and Zoom) and Bugcrowd (partnered with National Australia Bank, HP, FCA, and Motorola). Examples of reward programmes for privately disclosing vulnerabilities are Zero Day Initiative (ZDI) and Pwn2Own (trusted by Google, Apple, Microsoft, Lenovo and many more).

[8] Thomas and Beresford (2016) focus on the incentives of vendors in developing updates to fix vulnerabilities. They observe that these incentives relate to the vendors' business model. While they arise naturally in the case the business model is rent-based - users can switch provider if the product is not updated - vendors' reputation may provide appropriate incentives in the case products are purchase on a one-off basis. In a study on IoT products, Morgner et al. (2020) propose a regulatory framework to restore the incentives of vendors' incentives. Specifically, the authors propose mandatory security update labels informing consumers about the willingness of the manufacturer to provide security updates in the future. Maurushat and Nguyen (2022) argue for imposing legal obligations on vendors to correct known vulnerabilities promptly.

optimal, though hard to achieve without coordinated mechanisms like cost-sharing or liability rules.

Users' patching behaviour. Many successful cyberattacks result from users failing to install available updates. August et al. (2019) cite the WannaCry and NotPetya incidents, where patches had been released months in advance. Users often delay updates due to concerns about system instability or lack of awareness. Cognitive limitations may also play a role in limiting users' patching; Acquisti et al. (2018) observe that users rarely prioritise security and privacy. In addition, low levels of patching by users may depend on their failure to account for the positive externality of higher security for the other users of the same system.

August and Tunca (2006) compare alternative policies to manage network security in the presence of negative externalities and costly user patching: mandatory patching, where users are required to install patches; patching rebates, where the vendor compensates users for the cost of patching; and usage tax, where a tax on software usage can control the negative externalities caused by users who do not patch. Their findings suggest that rebate-based mechanisms tend to perform best in welfare terms, although the welfare-maximising alternative depends on the extent of patching costs, security risks, and whether the software is proprietary or open source. In a later paper, August et al. (2019) propose an alternative remedy: the "sale of patching rights". Consumers can pay a premium to retain patching autonomy, while those opting for automatic updates receive a discount. This segmentation improves patching rates while respecting user preferences.[9]

3.3 Reporting incentives and the role of top management

A growing body of literature explores the factors influencing firms' decisions to disclose cyber incidents, with particular focus on the role of top management. Managers with IT expertise can both improve a firm's cybersecurity posture and influence disclosure strategies. On one hand, managers with IT backgrounds may adopt effective technical solutions and strengthen resilience (Ford et al., 2022). On the other hand, they may strategically delay disclosure to avoid reputational damage or personal accountability (Foerderer and Schuetz, 2022; Amir et al., 2018). Indeed, Banker and Feng (2019) note that top executives—being closely tied to a firm's strategic direction—may be reluctant to disclose incidents that could harm performance or implicate leadership.[10]

Nonetheless, various studies highlight a positive role for cyber-aware executives. Ford et al. (2022) underline positive market reactions to the appointment of apical figures responsible for digital security, with a similar positive impact on the consequences of a security breach (Zafar et al., 2016). Other studies have identified the presence of managers with cyber-management tasks (or IT backgrounds) as a

[9] August et al. (2022) examine a different aspect of consumer behavior. Consumers can be heterogenous in their willingness to pay the ransom in the event of an attack. This has implications for the equilibrium market size and the vendor's profit, which may actually increase with the ransom demand.

[10] The authors find that there is positive correlation between CIO turnover and security breaches, with an increase in CIOs' departure after the notification of a security breach resulting from a system failure.

mitigating factor against cyber risk exposure (Haislip et al., 2017; Feng and Wang, 2019; Wang et al., 2023). Fleury and Salva (2025), using global data from the CISSM Cyberattacks Database, observe that the financial and reputational impact of breaches has declined over time, likely due to improved preparedness of firms. Overall, these findings emphasise the importance of corporate risk management strategies and highlight the need to prioritise cost recovery, recovery planning and context-specific trust restoration efforts.

Smith et al. (2021) reveal an opposite result; using hand-collected data on S&P 500 firms from 2005 to 2014, they show that companies with Chief Information Officers (CIOs) are more likely to be attacked by hackers. This may reflect either a greater likelihood of detection and disclosure or a higher exposure due to operating in risk-prone industries. The authors also suggest that firms lacking CIOs may fail to detect or report breaches altogether. More broadly, organisational culture and leadership play a crucial role. Ejjami (2024), in a study on French SMEs, highlights that effective cybersecurity depends not only on technical defences but also on cultivating awareness and proactive engagement across all levels of the organisation. Leaders who prioritise employee training and foster a culture of shared responsibility manage cyber risks more effectively.

4 The economic and financial impact of cyber risk

The growing frequency of cyberattacks has intensified concerns about their economic and financial repercussions for businesses, public institutions, and individuals. Estimating these losses is inherently difficult, especially when intangible factors like reputational damage or disruptions to services (e.g., in healthcare) are involved. Still, rough estimates place the global cost of cyber risk above $200 billion annually (Jamilov et al., 2023). For Italian firms with at least 20 employees, Biancotti (2017b) reports that direct costs from cyber incidents—such as operational disruptions or overtime pay—can reach €10,000, with some cases exceeding €200,000. Schlackl et al. (2022), in a meta-analysis of data breach literature, categorise the consequences of cyberattacks into internal effects (affecting the breached firm) and external effects (impacting customers, competitors, suppliers, and other stakeholders). In this section, we examine the literature on the economic and financial impact of cyberrisk. Table 4 summarizes the main results.

4.1 Effects on sales and consumption

Cyberattacks can affect a firm's sales through two main channels. First, they can influence consumers' perception of risk, increasing awareness and altering purchasing behaviour (Aivazpour et al., 2018), with effects that vary by demographic group. Older consumers tend to react more strongly (Chakraborty et al., 2016), a finding which is consistent with generational differences in risk aversion and privacy concerns (Grimes et al., 2010; Goldfarb and Tucker, 2012).

Table 4 Economic and financial impacts of cyber risk

Contribution	Focus	Approach	Key Results
Chakraborty et al. (2016)	Sales and consumption	Empirical (survey)	Older adults show stronger negative reactions in online retail; age moderates consumer response to breaches
Turjeman and Freinberg (2024)	Sales and consumption	Empirical	Data breach on extramarital dating site reduced activity and increased privacy-related behaviour
Berezina et al. (2012)	Sales and consumption	Experimental (survey)	Breaches decrease perceived service quality, satisfaction, and revisit intentions in the hospitality industry, regardless of whether financial data is exposed
Janakiraman et al. (2018)	Sales and consumption	Empirical (DiD)	In U.S. retail, 30% spending drop post-breach; effect mitigated for brand-loyal customers
Goel and Shawky (2009)	Short-term financial effects	Empirical (event study)	Stock prices drop following breach news; a rapid response can reduce investor panic
Spanos and Angelis (2016)	Short-term financial effects	Empirical (event study)	Consistent short-term loss in firm value; average cumulative abnormal returns (CARs) are significantly negative after the breach
Chang et al. (2020)	Long-term financial effects	Empirical (longitudinal analysis)	Stock value decline of publicly traded firms can persist up to 36 months; severity of breach and preventability matter
Huang and Wang (2021)	Long-term financial effects	Empirical	After a breach, firms face stricter loan terms, higher interest rates, and more collateral requirements. Impact is stronger for data-intensive firms
Martin et al. (2017)	Market spillovers	Empirical (event study)	Minor breaches cause negative spillover to rivals; major breaches trigger positive competitor effects due to customer switching.

A second channel through which cyber crimes affect sales is the erosion of consumer trust, with consequences for user engagement and loyalty (Lulandala, 2020).[11] Turjeman and Freinberg (2024), examining a major breach on a dating platform for extramarital affairs, find that affected users significantly reduce activity and information sharing post-incident. Similarly, in the context of the hotel industry, Berezina et al. (2012) show that hospitality customers report lower satisfaction and revisit intentions after a breach, regardless of whether they were directly impacted.

However, the gap between stated and actual consumer behaviour may be significant (Nofer et al., 2014). Based on a questionnaire with more than 2,600 respondents, Ablon et al. (2016) show that only 11% of them stopped dealing with the company after a breach. In contrast, Janakiraman et al. (2018), using transactional data from a U.S. department store, find a 30% spending drop among affected customers, though the effect is mitigated among brand-loyal clients.

In healthcare, Kwon and Johnson (2015) use data from more than seven hundred U.S. hospitals and show that while short-term effects like appointment cancellations

[11] In the wake of a data breach, organisations may implement a range of compensation strategies to rebuild consumer trust. For e-commerce platforms, these strategies may include issuing public apologies, offering identity theft protection and credit monitoring (Muzatko and Bansal, 2023). Nevertheless, the efficacy of these strategies is not homogenous across consumers, hence tailoring the compensation to the suffered wrongdoing and to consumer characteristics becomes crucial to mitigate the adverse effects of trust erosion through compensation (Kude et al., 2017).

may be limited, long-term impacts on outpatient visits and admissions can be substantial, particularly in competitive markets. Telang and Wattal (2007) identify similar dynamics in the software industry, with smaller firms suffering larger losses in market share.

The nature of the compromised information also matters. Using experimental data from more than two hundred U.S. participants, Labrecque et al. (2021) highlight that breaches involving personally identifiable information (e.g., Social Security numbers) generate more stress, but breaches of anonymous data (e.g., browsing habits) lead to stronger protective and switching behaviours. Other studies confirm that consumer responses vary depending on the type and sensitivity of the information (Acquisti et al., 2022; Markos et al., 2023; Slepchuk et al., 2021).

4.2 Short-term financial effects

A substantial body of research has documented a negative correlation between the announcement of cyberattacks and subsequent stock price movements (Goel and Shawky, 2009; Gordon et al., 2011; Hinz et al., 2015; Spanos and Angelis, 2016). This reaction reflects multiple concerns: erosion of customer trust (Campbell et al., 2003), regulatory fines (Gwebu et al., 2018), and the high costs of breach response and remediation efforts (Chen et al., 2012; Kamiya, 2021). Indeed, Fleury and Salva (2025) find evidence suggesting that investors anticipate increased future costs, more than immediate sales losses.

The severity of cyberattacks influences the magnitude of stock price declines (Chang et al., 2020; Rosati et al., 2017). Employing an event study methodology, Malhotra and Malhotra (2011), using data with public reports of breaches worldwide since 2000, find that larger data leaks lead to stronger market value depreciation. They argue that breaches involving client data should be interpreted as service failures due to their reputational and legal implications.

Other factors also shape market reactions. The type of attack is particularly relevant. Vergara Cobos and Selcen (2024) highlight that different asset types targeted by attacks lead to varying financial impacts. DDoS attacks, for example, often trigger strong shareholder backlash (Yayla and Hu, 2011; Benaroch et al., 2012; Eling, 2023), and their costs grow over time despite swift containment. A report by CISA (2020) estimates that the cost of a DDoS attack can reach $40,000 per hour for the victim, while costing the attacker as little as $1000 per day.

Kamiya (2021) reveals that breaches involving personal data reduce shareholder value by 1.09% within three days and can result in shareholder wealth losses of up to $1.2 billion due to direct 'out-of-pocket costs' (e.g. investigation and remediation costs, legal penalties and regulatory penalties). Similarly, Akey et al. (2024), using data from 18 different breach databases for the period 2005–2016 in the US, find that brand value declines by 5.6% on average. Piccotti and Wang (2022) show that breaches involving hacked portable devices significantly depress stock returns.

Top management characteristics also matter. Zafar et al. (2016), analysing over 400 incidents in the Lexis/Nexis database, highlight that having a Chief Information Officer (CIO) helps mitigate the negative impact on Tobin's Q by enabling quicker and more effective responses to attacks.

Industry context is another key moderator. Firms in finance and e-commerce suffer steeper declines in stock prices after breaches due to the sensitivity of the data they handle (Colivicchi and Vignaroli, 2019; Das et al., 2012; Tweneboah-Koduah et al., 2020). In such sectors, breaches can damage reputations and even trigger customer runs (Makridis, 2021; Cavusoglu et al., 2004).

Florackis et al. (2023) show that stock returns of firms highly exposed to cybersecurity risk outperform their peers under normal conditions, but underperform during periods of elevated cyber risk.

Finally, evidence on firms supplying cybersecurity services is mixed. Cavusoglu et al. (2004) and Chen et al. (2012) show that cybersecurity developers and IT consultants may experience short-term stock price gains following breaches, likely due to increased demand for their services. However, Chen et al. (2012) also find that larger breaches (measured by data lost) can negatively affect IT consultants' market value, suggesting that exposure to failures can undermine perceived competence.

4.3 Long-term financial impact of cyber risk

While the short-term financial impact of security breaches is well documented, the long-term effects remain less explored, and the evidence is mixed. Some studies suggest limited long-term consequences. For instance, Avery (2021) finds no significant effect on firm performance in the four quarters following an attack. Hovav and D'Arcy (2005), using an event study approach on data on virus public announcements between 1988 and 2002, observe that the market reacts negatively in about half of the cases. However, such a reaction vanishes over time and is limited to announcements involving IT products that contain computer viruses.

Conversely, Chang et al. (2020) analyse data breach news involving publicly traded companies and reveal that the negative impact on market valuation can persist for up to 36 months. Similar findings are reported by Morse et al. (2011) and Akey et al. (2024), who also note stronger effects when the breach was preventable with reasonable safeguards.

One challenge in assessing long-term impact lies in firms' evolving strategies and changing consumer attitudes. Gordon et al. (2011) observe a mitigation in the negative impact of breaches on stock prices after the 9/11 attacks, attributing this to improved recovery plans and a reduced tendency to avoid doing business with breached firms. Kamiya et al. (2021), using data on breach events from the Privacy Rights Clearinghouse in the period 2005–2017, confirm that breaches often reduce shareholder wealth, though the magnitude varies depending on public perception, sales expectations, and pre-breach risk management.

Investor behaviour also complicates the assessment of long-term effects. Hovav and Gray (2014) suggest that investors may adopt a "wait-and-see" approach, delaying decisions until more information is available. This may result in varied firm responses: some firms respond transparently and quickly (Gwebu et al., 2018; Gatzlaff and McCullough, 2010), while others delay action, possibly eroding investor confidence, resulting in a more significant decline in stock price (Johnson et al., 2017).

Another potential confounding factor relates to how cyber risk influences a firm's attitude toward innovation. The evidence here is also inconclusive. Akey et al. (2024) identify no clear effect on IT investment by targeted firms. He et al. (2019), analysing breaches from 2005 to 2014, report a 10% drop in R&D spending post-breach, particularly among firms with initially low R&D intensity. In contrast, Tosun (2021), extending the analysis to 2019, shows that breached firms tend to increase R&D investments, suggesting a strategic shift toward long-term resilience.

Several studies also assess the impact of cybersecurity on firms' access to credit. Kim et al. (2018), analysing over 4,000 loan facility-years, find that firms with strong IT reputations enjoy better loan conditions and face fewer rating downgrades. Similarly, Berkman et al. (2018) show that investors value firms with strong IT governance and experience in handling breaches. In contrast, Huang and Wang (2021), using a difference-in-differences approach, highlight that breached firms face higher loan spreads, stricter covenants, and more collateral requirements. These findings suggest that cybersecurity incidents can significantly affect a firm's cost of capital and access to financing.

4.4 Market spillovers

The literature examining the effects of cyberattacks also explores whether these effects extend beyond the directly affected firms. Choi et al. (2019) suggest a positive impact on the stock prices of competitors; these positive effects are driven by investor and consumer behaviour shifting away from breached firms toward companies perceived as having stronger cybersecurity practices (Jeong et al., 2019; Crosignani et al., 2022). Conversely, Osei-Bryson et al. (2012), using a dataset in which breached firms are matched with their industry rivals, find evidence of intra-industry contagion. This result is consistent with more recent findings by Kamiya et al. (2021), who suggest that the negative sentiment surrounding a breach often spreads to rival firms, as news of security vulnerabilities tends to cast a shadow over the entire industry. Interestingly, the severity of security breaches can influence whether the impact on rival firms is positive or negative. Using the D&B Hoover's database, Martin et al. (2017) match breached firms with their closest publicly listed competitors and show that less severe incidents tend to generate negative spillovers. This effect is driven by concerns that similar breaches could potentially affect rival firms. However, as the severity of the attacks increases, consumers become more likely to shift away from the breached firm toward its competitors, resulting in positive spillovers for the latter.

5 Cybersecurity enhancing regulation

Governments worldwide are intensifying regulatory efforts to bolster cybersecurity across the public and private sectors.[12] These efforts combine mandatory measures—such as incident reporting requirements and risk management obligations—with vol-

[12] The EU has taken a particularly proactive stance, designing a comprehensive framework that builds on the foundation of the GDPR's mandatory breach reporting (Art. 33) and the NIS Directives, and that

untary initiatives, including cybersecurity certifications and staff training programs. The EU exemplifies this dual approach: the Cybersecurity Act introduces a voluntary certification framework, while the Cyber Resilience Act imposes binding requirements on manufacturers regarding product security, vulnerability management, and software updates. This section examines the diverse regulatory instruments studied in the academic literature, particularly focusing on the role of liability rules, disclosure mandates, behavioural nudges, and cyber insurance in shaping cybersecurity outcomes. The most relevant studies are presented in Table 5.

5.1 Liabilities and security standards

The debate around using liability to incentivise cybersecurity—especially in software markets—is long-standing.[13] Without liability, developers may underinvest in security since end-users often bear the consequences of attacks (Varian, 2000; Sager & Green, 2002). However, excessive liability could stifle innovation by increasing compliance costs (Anderson, 1994; Moore, 2010), to the extent that the burden of implementing a liability regime might outweigh the overall benefits (Fryer et al., 2013). Given that software is inherently prone to bugs, Moore (2010) warns that blanket liability is no panacea.[14]

A few theoretical studies explore these dynamics in greater detail. Kim et al. (2011) show that liability incentivises a monopolistic software vendor to invest in security only when the damages suffered by consumers in the event of an attack are heterogeneous. Conversely, when damages are homogeneous, liability merely results in higher prices. De Cornière and Taylor (2024) highlight that optimal liability mechanisms depend on business models: platforms relying on advertising revenues benefit more from mixed approaches combining fines and partial liability.

Other scholars underscore the importance of standards to improve cybersecurity (e.g., Pym et al., 2013; Gordon et al., 2015).[15] Lam (2016) proposes a combined approach: using standards to stimulate observable security investments and complementing them with partial liability to incentivise unobservable efforts, such as identifying and fixing vulnerabilities. In a more recent work, Lam and Seifert (2023) show that policy effectiveness also depends on the interdependence between privacy and security choices, as firms' data-sharing behaviour affects their security investments. Lee et al. (2016) hold a different view and warn against potential drawbacks of this policy instrument. Since standards can only address certain aspects of cybersecurity,

will be shaped by the Cyber Resilience Act. The UK opted for a similar approach, implementing the Data Protection Act early on and embracing the same NIS Directives. More recently, it adopted the Cyber Essentials, a government-backed set of cybersecurity standards that organizations are encouraged to follow. Differently from the EU organic approach, the U.S. regulatory framework builds on multiple laws that vary by state, industry and type of data stored.

[13] Ciet and Verdier (2023) study the role of liabilities and other policy tools in the context of cybersecurity of payment services.

[14] Bellovin (2023) warns against the negative effects for open source software, suggesting that liabilities would drastically reduce the incentives of open source developers to share software code.

[15] De Cornière and Taylor (2024) and Huang et al. (2024) discuss the role of less intrusive regulations such as security certification by independent agencies or audits.

Table 5 Policy tools and regulations

Contribution	Literature Stream	Approach	Key Results
Kim et al. (2011)	Liability and standards	Theoretical	With a monopolistic software vendor, liabilities are effective in increasing security investment only if consumer damages are heterogeneous
Lam (2016)	Liability and standards	Theoretical	The combination of a policy of partial liability and minimum standards achieves the first-best outcome.
Lee et al. (2016)	Liability and standards	Theoretical	Tighter standards may not increase security due to limited scope and compliance used to reduce liabilities.
Lam and Seifert (2023)	Liability and standards	Theoretical	Interdependency between privacy and security affects policy effectiveness. Firms tend to under-invest in security and over-share data.
August and Tunca (2011)	Liability and standards	Theoretical	Under network externalities among users, standards work best when zero-day risk is low; patching liabilities are better when high; damages liability is least effective
De Cornière and Taylor (2024)	Liability and standards	Theoretical	Optimal policies depend on the business model (price vs. ad-based) of competing platforms offering differentiated products. A mix of fines and liabilities is optimal to incentivise security investments for advertising-based business models.
Shackelford et al. (2022)	Liability and standards	Empirical (survey)	SMEs struggle with compliance. Security doesn't always improve with tighter standards.
Romanosky et al. (2011)	Data breach disclosure laws	Empirical (Quasi-experimental)	Disclosure laws reduce identity theft from breaches by 6.1%.
Sen and Borle (2015)	Data breach disclosure laws	Empirical	Disclosure laws reduce breach risk at the industry level (not state level), especially in financial, education, and medical sectors.
Bosiako and Keefe (2021)	Data breach disclosure laws	Empirical (DiD)	Firms respond to disclosure laws by increasing cash holdings to hedge greater risk.
Florackis et al. (2023)	Cyber insurance	Empirical and text analysis	Propose a novel firm-level measure of cybersecurity risk and show that it correlates with cyber insurance adoption
Acquisti et al. (2018)	Nudging security	Literature review	Personalised nudges and reminders increase patching and safe behaviour.

firms may pay less attention to areas that fall outside the scope of regulation. Moreover, companies might use compliance with standards to limit their liability in the event of a breach.

In a theoretical analysis, August and Tunca (2011) compare three policy tools: damage liability for losses caused by cyberattacks, patching liability — where the vendor compensates users for patching costs — and security standards. Their findings suggest that standards are most effective when zero-day risks are low, while patching liability is preferable in high-risk scenarios. Damage liability alone is generally less effective in improving social welfare.

Empirical evidence on the impact and effectiveness of these policy tools is limited. Shackelford et al. (2022) analyse survey data from 197 U.S. organisations. According to their study, SMEs may find it challenging to comply with regulations, particularly when standards are poorly defined. Additionally, critical infrastructure firms are more likely to adopt established frameworks, such as those developed by the National Institute of Standards and Technology (NIST).

5.2 Data breach disclosure laws

Cyber incidents are frequently underreported and only a fraction reach the public domain or are disclosed to government authorities (Amir et al., 2018; Biancotti, 2017a).[16] Disclosure laws aim to address this opacity by requiring firms to notify affected individuals when their personal data is compromised. These provisions offer several benefits. They enhance companies' ex-ante incentives to invest in security, prevent breaches, and protect their reputation. In the event of a security breach, notified individuals can take timely mitigation measures to limit potential harm. In addition, greater public disclosure of information on criminal incidents provides valuable insights to researchers, government agencies, and insurance companies, helping them better understand attack targets and the strategies employed by hackers.

Evidence on the effectiveness of mandatory disclosure is promising. Romanosky et al. (2011), exploiting the difference between U.S. states' mandatory disclosure adoption and the timing of adoption, highlight that mandatory disclosure laws reduce identity theft from cyber breaches by 6.1%. Sen and Borle (2015) show industry-level risk reductions, particularly in finance, education, and healthcare sectors. However, disclosure mandates can increase firms' perceived risk, with possible unintended consequences. Bosiako and Keefe (2021) use a difference-in-differences approach to examine how U.S. firms adjust their financial decisions in response to changes in state-level data breach disclosure laws. They show that firms subject to such laws increase cash holdings —likely as a hedge against legal and reputational fallout— suggesting that disclosure requirements influence not only security posture but also corporate financial behaviour.

5.3 Nudging security

As highlighted in Sect. 3, behavioural biases—such as neglecting software updates—remain a major cybersecurity vulnerability. Human error, related to phishing and credential misuse, plays a role in nearly 70% of breaches (Verizon, 2024).

Nudge theory provides a promising strategy for subtly influencing user behaviour towards security best practices.[17] Studies show that simple interventions—such as risk-focused messages (Acquisti et al., 2018), strong password prompts (Hartwig and Reuter, 2021; Zou et al., 2024), or visual cues like colour-coded labels (Jeske et al.,

[16] For instance, the U.S. Federal Bureau of Investigation reported that fewer than 20% of companies affected by the Hive ransomware informed the U.S. government of the attack (Daniel, 2023).

[17] More intrusive interventions such as priming users with cybersecurity risks can have unintended consequences, such as inducing a more risk-averse behaviour (Sharma et al., 2021).

2014)—can significantly improve user behaviour. Techniques like gamification and salience have also been shown to enhance engagement (Dodge et al., 2023; Kankane et al., 2018). Personalised nudges are particularly effective. Peer et al. (2019) report that tailored nudges are up to four times more successful than generic ones. However, over time, users may become desensitised to frequent prompts (Zimmermann and Renaud, 2021). To sustain long-term effectiveness, nudges can be combined with complementary tools such as reminders or commitment devices (Frik et al., 2018).

5.4 Mandatory cyber insurance

The market for cyber insurance is a relatively small segment of the broader commercial property and liability insurance sector, with adoption rates averaging around 30% in most economies and remaining in the single digits among small and medium-sized enterprises (OECD, 2017). These figures are worrying, given the rising frequency of cyber incidents and their potential to cause substantial losses (Shevchenko et al., 2023).

Several factors hinder the development of an efficient cyber insurance market. First, cyber risks are often correlated across firms due to shared technologies and common vulnerabilities (Awiszus et al., 2023). This correlation undermines the principle of independent risk necessary for effective insurance pooling (Marotta et al., 2017). It also exacerbates moral hazard concerns and limits risk diversification (Arce et al., 2024; Baker and Shortland, 2022; Dou et al., 2020; Yin et al., 2023). One proposed solution is a government-backed backstop mechanism designed to hedge against large-scale attacks and protect against systemic risk (Association of British Insurers, 2017; Smith, 2023). However, such a mechanism must be carefully framed to incentivise proactive risk management and avoid fostering complacency (EIOPA, 2018).

Second, a small pool of insured entities limits diversification, thereby reducing the insurer's ability to lower premiums. Introducing a mandatory cyber insurance scheme could mitigate individual business exposure and strengthen overall cyber resilience (Miller, 2019; Patterson, 2020; Woods and Moore, 2020). Proponents argue that, if properly enforced, mandatory coverage would broaden the insurance base and help reduce premiums. A mandatory scheme could also help clarify certain legal grey areas, particularly those regarding coverage for ransom payments and administrative fines (Swiss Re, 2017; Lemnitzer, 2021; Matheson, 2019). The effective implementation of mandatory coverage would require the adoption of complementary measures. Woods and Simpsons (2017) emphasise the need for minimum insurance standards. Since cyber policies are typically customised, establishing a baseline would help ensure that even smaller firms—often lacking the capacity for thorough security assessments—receive adequate protection (Franke, 2017). Minimum requirements should also be defined for policy content, including guaranteed support services, clear coverage definitions, and limitations on contentious claims, particularly those involving ransom payments to cybercriminals. Clear regulatory guidance would enhance transparency, standardisation, and consumer protection.

Finally, a major barrier to market efficiency is the difficulty of accurately assessing firm-level cyber risk.[18] Lemnitzer (2021) highlights the need for improved data sharing and a centralised claims database. Facilitating information exchange among insurers would enhance risk modelling and improve premium accuracy. A relatively low-cost solution could involve linking data-sharing obligations to existing incident reporting duties under the GDPR (Art. 33), the NIS directives, and the new Cyber Resilience Act.

6 Conclusions

Cyber risk has become one of the most pressing challenges for businesses, governments, and individuals. The growing reliance on digital infrastructures, coupled with the rising sophistication of cyberattacks, has escalated both the frequency and the severity of breaches. Global estimates suggest that the cost of cybercrime could have surpassed 8 USD trillion in 2023 (Fleck and Richter, 2024), impacting financial markets, consumer trust, and critical infrastructures. This phenomenon not only threatens economic stability but also poses a significant risk to national security, highlighting the urgent need for comprehensive cybersecurity strategies.

This survey reviews the economic literature on cyber risk, focusing on the drivers of hackers, firms, and users' behaviour, the impact on markets, and the policy implications. The complexity of the phenomenon calls for an interdisciplinary approach that combines economic analysis with insights from information security, management, and behavioural sciences.

Our review highlights several interesting aspects of cyber risk. The perception of hackers as a homogeneous group is misleading. In reality, hackers differ significantly in their motivations, skill levels, targets, and attack strategies. This heterogeneity has important implications for the design of effective defensive strategies. Technological advancements, such as the rise of AI, further complicate the picture as they represent both a blessing and a curse: on the one hand, they enhance defence capabilities through better threat detection and faster response; on the other hand, they enable increasingly sophisticated and harder-to-detect attacks. Quantifying the damages caused by cyberattacks is challenging, in part because they often involve intangible elements. Nevertheless, a relatively well-developed body of research documents a short-term negative correlation between the announcement of cyberattacks and the subsequent stock price movements of the affected firms. Under certain conditions, the impact of an attack may even spill over to other companies within the same sector. By contrast, evidence on longer-term consequences is more limited and harder to interpret, given the presence of confounding factors and firms' strategic behaviour.

A central theme in the literature is the role of incentives in shaping cybersecurity outcomes. Security failures are often the result of misaligned incentives among the various actors involved in prevention and response. Externalities—both technical and market-related—distort the incentives of vendors and system developers to invest in

[18] Relatedly, another challenge to increase insurance coverage is the lack of a clear definition of cyber risk. Florackis et al. (2023) propose a firm-level risk metric based on textual analysis.

protection at socially efficient levels. The rapid pace of technological development in the digital realm requires constant vigilance: vulnerabilities must be identified on an ongoing basis, and patches must be developed and deployed promptly. Users play a critical role in this ecosystem; however, behavioural limitations or concerns about system crashes can delay the installation of critical updates, undermining overall system security.

To address these issues, a growing body of literature has explored the potential of policy tools aimed at aligning private incentives with socially optimal levels of cybersecurity investment. In particular, liability regimes have received considerable attention. In the absence of liabilities, vendors and developers lack incentives to enhance the security of their products. However, liabilities must be carefully designed to avoid stifling innovation. Several studies have also examined the effects of data breach disclosure laws. These provisions can incentivise better security practices and allow users to adopt timely mitigation strategies in the aftermath of an attack. Taken together, the literature underscores the importance of carefully designed liability regimes, the strategic role of disclosure obligations, and the need for regulatory approaches that account for market structure, business models, and interdependencies within digital ecosystems. Effective cybersecurity governance also requires coordination across networked systems and a better alignment between private incentives and collective resilience.

Based on our survey, we identified several gaps in the literature that deserve further investigation. First, modelling hackers' behaviour remains underdeveloped. As just mentioned, the literature treats hackers as a relatively homogenous group, overlooking the diversity of their motivations and strategies. There is a pressing need for more nuanced models that capture the varying profiles of attackers, ranging from cybercriminals driven by financial incentives to state-sponsored actors with political motives. Understanding these differences is crucial for designing targeted and effective defence strategies.

Second, underreporting and partial awareness of threats by users and businesses limit and skew data availability. As a consequence, evidence on the drivers and effects of cyber risk is still relatively scant. Enhancing data availability through better detection mechanisms and regulatory requirements for disclosure is essential to improving empirical research and risk assessment models, and fully understanding the true scope of cyber risk.

Third, most studies concentrate on the immediate effects of cyberattacks, such as stock price drops, short-term financial losses, or reduction of sales. There is relatively limited research on the long-term consequences of cyber incidents. For example, there is potential to investigate whether cyber threats drive firms to innovate more rapidly or hinder progress due to increased security costs. Future research should explore how cyber risk can shape market structures and innovation over time.

Fourth, while regulations like data breach disclosure laws, cybersecurity standards, and initiatives like bug bounty programmes are becoming more common, their effectiveness has yet to be thoroughly studied. Research is needed to understand how these regulations influence firms' cybersecurity strategies and market dynamics in the long run, particularly in industries with high data sensitivity, such as finance and healthcare.

Finally, the literature has yet to fully explore how the welfare cost of cyber risk is distributed across firms and consumers and how insurance mechanisms or regulatory measures might mitigate the impact on vulnerable groups. Addressing these questions is critical for ensuring that the financial and social costs of cyber incidents do not disproportionately affect consumers.

Although the economics of cybersecurity still presents several open questions, it is clear that a multidisciplinary approach is essential to address the complex and evolving landscape of cyber risk. The dynamic nature of these risks demands a continuous adaptation of corporate strategies and regulatory policies. In turn, the increasing integration of artificial intelligence, the Internet of Things (IoT), and other emerging technologies into business operations adds new layers of vulnerability that need to be addressed. Future research is essential to improve our understanding and better address the complexities of cyber threats as technological innovations accelerate.

Funding Open access funding provided by Politecnico di Torino within the CRUI-CARE Agreement.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

Ablon, L., Heaton, P., Lavery, D., & Romanosky, S. (2016). Consumer attitudes toward data breach notifications and loss of personal information. In RAND Corporation eBooks. https://doi.org/10.7249/rr1187

Acemoglu, K. D., Malekian, A., & Koksal, A. E. (2016). Network security and contagion. https://dspace.mit.edu/handle/1721.1/119662

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2018). Nudges for privacy and security. *ACM Computing Surveys*, *50*(3), 44. https://doi.org/10.1145/3054926

Acquisti, A., Brandimarte, L., & Hancock, J. (2022). How privacy's past May shape its future. *Science*, *375*(6578), 270–272. https://doi.org/10.1126/science.abj0826

Aivazpour, Z., Valecha, R., & Chakraborty, R. (2018). The impact of data breach severity on Post-Breach online shopping intention. International Conference on Information Systems. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1218%26context=icis2018

Akey, P., Lewellen, S., Liskovich, I., & Schiller, C. (2024). Hacking corporate reputations. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3143740

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability*, *60*, 100989. https://doi.org/10.1016/j.jfs.2022.100989

Algarni, A. M., & Malaiya, Y. K. (2014). Software vulnerability Markets: discoverers and buyers. *Zenodo (CERN European Organization for Nuclear Research)*. https://doi.org/10.5281/zenodo.1091516

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. https://doi.org/10.1007/s11142-018-9452-4

Anderson, R. J. (1994). Liability and computer security: Nine principles. In Lecture notes in computer science (pp. 231–245). https://doi.org/10.1007/3-540-58618-0_67

Anderson, R. (2001). Why information security is hard - an economic perspective. Proceedings of the Seventeenth Annual Computer Science Applications Conference. New Orleans: IEEE, pp.358–365. https://doi.org/10.1109/acsac.2001.991552

Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, *314*(5799), 610–613. https://doi.org/10.1126/science.1130992

Arce, D. G. (2018). Malware and market share. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy010

Arce, D., Woods, D. W., & Böhme, R. (2024). Economics of incident response panels in cyber insurance. *Computers & Security*, *103742*. https://doi.org/10.1016/j.cose.2024.103742

Arora, A., Caulkins, J. P., & Telang, R. (2006). Research note—sell first, fix later: Impact of patching on software quality. *Management Science*, *52*(3), 465–471.

Association of British Insurers [ABI] (2017). Evidence on Cyber Security. In https://committees.parliament.uk/writtenevidence/78053/pdf/. Retrieved September 26, 2024, from https://committees.parliament.uk/writtenevidence/78053/pdf/

Atefi, S., Sivagnanam, A., Ayman, A., Grossklags, J., & Laszka, A. (2023). The benefits of vulnerability discovery and bug bounty programs: Case studies of chromium and firefox. *Proceedings of the ACM Web Conference 2023 (WWW '23)*. https://doi.org/10.1145/3543507.3583352

August, T., & Tunca, T. I. (2006). Network software security and user incentives. *Management Science*, *52*(11), 1703–1720. https://doi.org/10.1287/mnsc.1060.0568

August, T., & Tunca, T. I. (2011). Who should be responsible for software security? A comparative analysis of liability policies in network environments. *Management Science*, *57*(5), 934–959. https://doi.org/10.1287/mnsc.1100.1304

August, T., Dao, D., & Kim, K. (2019). Market segmentation and software security: Pricing patching rights. *Management Science*, *65*(10), 4575–4597. https://doi.org/10.1287/mnsc.2018.3153

August, T., Dao, D., & Niculescu, M. F. (2022). Economics of ransomware: Risk interdependence and Large-Scale attacks. *Management Science*, *68*(12), 8979–9002. https://doi.org/10.1287/mnsc.2022.4300

Avery, A. (2021). After the disclosure: Measuring the short-term and long-term impacts of data breach disclosures on the financial performance of organizations. *Information & Computer Security*, *29*(3), 500–525. https://doi.org/10.1108/ics-10-2020-0161

Awiszus, K., Knispel, T., Penner, I., Svindland, G., Voß, A., & Weber, S. (2023). Modeling and pricing cyber insurance. *European Actuarial Journal*, *13*(1), 1–53. https://doi.org/10.1007/s13385-023-00341-9

Baker, T., & Shortland, A. (2022). Insurance and enterprise: Cyber insurance for ransomware. *The Geneva Papers on Risk and Insurance Issues and Practice*, *48*(2), 275–299. https://doi.org/10.1057/s41288-022-00281-7

Bandyopadhyay, T., Liu, D., Mookerjee, V. S., & Wilhite, A. W. (2014). Dynamic competition in IT security: A differential games approach. *Information Systems Frontiers*, *16*(4), 643–661. https://doi.org/10.1007/s10796-012-9373-x

Banker, R. D., & Feng, C. (2019). The impact of information security breach incidents on CIO turnover. *J Inform Syst*, *33*(3), 309–329.

Bellovin, S. M. (2023). Is cybersecurity liability a liability? *IEEE Security & Privacy*, *21*(4), 99–100. https://doi.org/10.1109/msec.2023.3273461

Benaroch, M., Chernobai, A., & Goldstein, J. (2012). An internal control perspective on the market value consequences of IT operational risk events. *International Journal of Accounting Information Systems*, *13*(4), 357–381. https://doi.org/10.1016/j.accinf.2012.03.001

Bencivelli, L., & Mongardini, M. (2024). Italian firms cybersecurity risk perception and mitigation strategies. Questioni di Economia e Finanza, Discussion paper no. 852. Banca d'Italia, Economic Research and International Relations Area.

Berezina, K., Cobanoglu, C., Miller, B., & Kwansa, F. A. (2012). The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. *International Journal of Contemporary Hospitality Management*, *24*(7), 991–1010. https://doi.org/10.1108/09596111211258883

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. S. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508–526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Bhushan, A., Billa, V., Sonkar, M., & Chavan, V. (2022). The Dynamics of a Bug Bounty Platform. *2022 5th International Conference on Advances in Science and Technology (ICAST)*. https://doi.org/10.1109/icast55766.2022.10039642

Biancotti, C. (2017a). Cyber attacks: Preliminary evidence from the bank of italy's business surveys. *Social Science Research Network*. https://doi.org/10.2139/ssrn.2954991

Biancotti, C. (2017b). The price of cyber (In)Security: Evidence from the Italian private sector. *Social Science Research Network*. https://doi.org/10.2139/ssrn.3082195

Bier, V., Oliveros, S., & Samuelson, L. (2007). Choosing what to protect: Strategic defensive allocation against an unknown attacker. *Journal of Public Economic Theory*, *9*(4), 563–587. https://doi.org/10.1111/j.1467-9779.2007.00320.x

Boasiako, K. A., & Keefe, M. O. (2021). Data breaches and corporate liquidity management. *European Financial Management*, *27*(3), 528–551. https://doi.org/10.1111/eufm.12289

Boston Consulting Group (2019). Global Wealth 2019: Reigniting Radical Growth. https://web-assets.bcg.com/img-src/BCG-Reigniting-Radical-Growth-June-2019_tcm9-222638.pdf

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market*. *Journal of Computer Security*, *11*(3), 431–448. https://doi.org/10.3233/JCS-2003-11308

Canann, T. J. (2019). Toward a theory of vulnerability disclosure policy: a hacker's game. In Decision and Game Theory for Security: 10th International Conference, GameSec 2019, Stockholm, Sweden, October 30–November 1, 2019, Proceedings 10 (pp. 118–134). Springer International Publishing.

Casey, E. (2003). Determining Intent-opportunistic vs targeted attacks. *Computer Fraud & Security*, *2003(4)*, 8–11. https://doi.org/10.1016/S1361-3723(03)04010-7

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 70–104. https://doi.org/10.1080/10864415.2004.11044320

Cavusoglu, H., Cavusoglu, H., & Zhang, J. (2008). Security patch management: Share the burden or share the damage? *Management Science*, *54*(4), 657–670. https://doi.org/10.1287/mnsc.1070.0794

Cerdeiro, D. A., Dziubiński, M., & Goyal, S. (2017). Individual security, contagion, and network design. *Journal of Economic Theory*, *170*, 182–226. https://doi.org/10.1016/j.jet.2017.05.006

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Raghav Rao, H. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems*, *83*, 47–56. https://doi.org/10.1016/j.dss.2015.12.007

Chang, K., Gao, Y., & Lee, S. (2020). The effect of data theft on a firm's Short-Term and Long-Term market value. *Mathematics*, *8*(5), 808. https://doi.org/10.3390/math8050808

Chen, J. V., Li, H. C., Yen, D. C., & Bata, K. V. (2012). Did IT consulting firms gain when their clients were breached. *Computers in Human Behavior*, *28*(2), 456–464. https://doi.org/10.1016/j.chb.2011.10.017

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*, 100167. https://doi.org/10.1016/j.chbr.2022.100167

Choi, J. P., Fershtman, C., & Gandal, N. (2010). Network security: Vulnerabilities and disclosure policy. *The Journal of Industrial Economics*, *58*(4), 868–894. https://doi.org/10.1111/j.1467-6451.2010.00435.x

Ciet, N., & Verdier, M. (2023). Cyber security and cloud outsourcing of payments. https://doi.org/10.2139/ssrn.4304898

CISA. (2020). *Cost of a cyber incident*. Systematic review and cross-validation.

Colivicchi, I., & Vignaroli, R. (2019). Forecasting the impact of information security breaches on stock market returns and VAR backtest. *Journal of Mathematical Finance*, *09*(03), 402–454. https://doi.org/10.4236/jmf.2019.93024

Comino, S., Fedele, A., & Manenti, F. (2025). *Cyber (in)security in digital services: The unintended effects of interability*. mimeo.

Cremonini, M., & Nizovtsev, D. (2006). Understanding and Influencing Attackers' Decisions: Implications for Security Investment Strategies. Workshop on the Economics of Information Security (WEIS), Robinson College, University of Cambridge, 26–28 June 2006. http://weis2006.econinfosec.org/docs/3.pdf

Cremonini, M., & Nizovtsev, D. (2009). Risks and benefits of signaling information system characteristics to strategic attackers. *Journal of Management Information Systems*, *26*(3), 241–274. https://doi.org/10.2753/MIS0742-1222260308

Crosignani, M., Macchiavelli, M., & Silva, A. F. (2022). Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics*, *147*(2), 432–448. https://doi.org/10.1016/j.jfineco.2022.12.002

Daniel, M. (2023). *Reporting cyberattacks will soon be mandatory*. Is your company ready. Harvard Business Review.

Das, S., Mukhopadhyay, A., & Anand, M. (2012). Stock market response to information security breach: A study using firm and attack characteristics. *Journal of Information Privacy & Security*, *8*(4), 27–55. https://doi.org/10.1080/15536548.2012.10845665

De Cornière, A., & Taylor, G. (2024). A model of information security and competition. *Marketing Science*, *0*, 0. https://doi.org/10.1287/mksc.2023.0513

Department for Digital, Culture, Media &, & Sport (2022). *Cyber security breaches survey 2022*. (2022, July 11). UK Government. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022

Dodge, C. E., Fisk, N., Burruss, G. W., Moule, R. K., & Jaynes, C. M. (2023). What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology & Public Policy*, *22*(4), 849–868. https://doi.org/10.1111/1745-9133.12641

Dou, W., Tang, W., Wu, X., Qi, L., Xu, X., Zhang, X., & Hu, C. (2020). An insurance theory based optimal cyber-insurance contract against moral hazard. *Information Sciences*, *527*, 576–589. https://doi.org/10.1016/j.ins.2018.12.051

Dziubiński, M., & Goyal, S. (2013). Network design and defence. *Games and Economic Behavior*, *79*, 30–43. https://doi.org/10.1016/j.geb.2012.12.007

Dziubiński, M., & Goyal, S. (2017). How do you defend a network? *Theoretical Economics*, *12*(1), 331–376. https://doi.org/10.3982/te2088

EIOPA (2018). Understanding cyber insurance—a structured dialogue with insurance companies. European insurance and occupational pensions authority. https://www.eiopa.europa.eu/publications/understanding-cyber-insurance-structured-dialogue-insurance-companies_en

Ejjami, R. (2024). The digital evolution: Strategies for overcoming cybersecurity and adoption challenges in French SMEs. *International Journal for Multidisciplinary Research*, *6*(3). https://doi.org/10.36948/ijfmr.2024.v06i03.21202

Eling, M., Elvedi, M., & Falco, G. (2023). The economic impact of extreme cyber risk scenarios. *North American Actuarial Journal*, *27*(3), 429–443. https://doi.org/10.1080/10920277.2022.2034507

ENISA (2023). Artificial intelligence and cybersecurity research. ENISA Research and Innovation Brief. https://www.enisa.europa.eu/sites/default/files/publications/Artificial%20Intelligence%20and%20Cybersecurity%20Research.pdf

Ettredge, M. L., & Richardson, V. J. (2003). Information transfer among internet firms: The case of hacker attacks. *The Journal of Information Systems/Journal of Information Systems*, *17*(2), 71–82. https://doi.org/10.2308/jis.2003.17.2.71

Europol (2025). *The changing DNA of serious and organised crime*. Publications Office of the European Parliament.

Fedele, A., & Roner, C. (2022). Dangerous games: A literature review on cybersecurity investments. *Journal of Economic Surveys*, *36*(1), 157–187. https://doi.org/10.1111/joes.12456

Fedele, A., Tonin, M., & Valerio, M. (2024). Phishing attacks: An analysis of the victims' characteristics based on administrative data. *Economics Letters*, *237*, 111663. https://doi.org/10.1016/j.econlet.2024.111663

Feng, C., & Wang, T. (2019). Does CIO risk appetite matter? Evidence from information security breach incidents. *International Journal of Accounting Information Systems*, *32*, 59–75. https://doi.org/10.1016/j.accinf.2018.11.001

Fleck, A., & Richter, F. (2024). Cybercrime expected to Skyrocket in coming years, Statista Daily Data. https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until2027/

Fleury, A., & Salva, C. (2025). How do Cyberattacks Impact Firms? Available at SSRN: https://ssrn.com/abstract=5175947 or https://doi.org/10.2139/ssrn.5175947

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. *The Review of Financial Studies*, *36*(1), 351–407. https://doi.org/10.1093/rfs/hhac024

Foerderer, J., & Schuetz, S. W. (2022). Data breach announcements and stock market reactions: A matter of timing? *Management Science*, *68*(10), 7298–7322. https://doi.org/10.1287/mnsc.2021.4264

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?? *The Review of Financial Studies*, *32*(5), 1798–1853. https://doi.org/10.1093/rfs/hhz015

Ford, A., Al-Nemrat, A., Ghorashi, S. A., & Davidson, J. J. (2022). Impact of CISO appointment announcements on the market value of firms. https://www.semanticscholar.org/paper/Impact-of-CISO-Appointment-Announcements-on-the-of-Ford-Al-Nemrat/cd8d233291fb400c5e7fbf8d1320d5f329babe3e

Franke, U. (2017). The cyber insurance market in Sweden. *Computers & Security*, *68*, 130–144. https://doi.org/10.1016/j.cose.2017.04.010

Frik, A., Egelman, S., Harbach, M., Malkin, N., & Péer, E. (2018). *Better Late(r) than Never: Increasing Cyber-Security Compliance by Reducing Present Bias*. Workshop on the Economics of Information Security (WEIS). https://blues.cs.berkeley.edu/blog/2018/06/29/better-later-than-never-increasing-cyber-security-compliance-by-reducing-present-bias-weis-18/

Fryer, H., Moore, R., & Chown, T. (2013). On the viability of using liability to incentivise internet security. https://www.semanticscholar.org/paper/On-the-Viability-of-Using-Liability-to-Incentivise-Fryer-Moore/5495cf43fe1cb784f62cdd33b6ece0d954f0f293

Gao, X., & Zhong, W. (2015). Information security investment for competitive firms with hacker behavior and security requirements. *Annals of Operation Research/Annals of Operations Research*, *235*(1), 277–300. https://doi.org/10.1007/s10479-015-1925-2

Gao, X., & Zhong, W. (2016). Economic incentives in security information sharing: The effects of market structures. *Information Technology and Management*, *17*(4), 361–377. https://doi.org/10.1007/s10799-015-0253-1

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review*, *13*(1), 61–83. https://doi.org/10.1111/j.1540-6296.2010.01178.x

Geer, D., Jardine, E., & Leverett, E. (2020). On market concentration and cybersecurity risk. *Journal of Cyber Policy*, *5*(1), 9–29. https://doi.org/10.1080/23738871.2020.1728355

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, *46*(7), 404–410. https://doi.org/10.1016/j.im.2009.06.005

Goldfarb, A., & Tucker, C. (2012). Shifts in privacy concerns. *The American Economic Review*, *102*(3), 349–353. https://doi.org/10.1257/aer.102.3.349

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457. https://doi.org/10.1145/581271.581274

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, *19*(1), 33–56. https://doi.org/10.3233/JCS-2009-0398

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, *1*(1), 3–17. https://doi.org/10.1093/cybsec/tyv011

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2018). Empirical evidence on the determinants of cybersecurity investments in private sector firms. *Journal of Information Security*, *09*(02), 133–153. https://doi.org/10.4236/jis.2018.92010

Goyal, S., & Vigier, A. (2014). Attack, defence, and contagion in networks. *Review of Economic Studies*, *81*(4), 1518–1542. https://doi.org/10.1093/restud/rdu013

Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older adults' knowledge of internet hazards. *Educational Gerontology*, *36*(3), 173–192. https://doi.org/10.1080/03601270903183065

Grossklags, J., Christin, N., & Chuang, J. (2008). Secure or insure? A game-theoretic analysis of information securitygames. Proceedings of the 17th International Conference on World Wide Web, 209–2018. https://doi.org/10.1145/1367497.1367526.

Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, *35*(2), 683–714. https://doi.org/10.1080/07421222.2018.1451962

Haislip, J. Z., Lim, J., & Pinsker, R. (2017). Do the Roles of the CEO and CFO Differ when it comes to Data Security Breaches? https://www.semanticscholar.org/paper/Do-the-Roles-of-the-CEO-and-CFO-Differ-when-it-to-Haislip-Lim/4cfafdff7956dd0d106342ca72cd42f9f17e014a

Harry, C., & Gallagher, N. (2018). Classifying cyber events: A proposed taxonomy. *Journal of Information Warfare*, *17*(3), 17–31. https://www.jstor.org/stable/26633163

Hartwig, K., & Reuter, C. (2021). Nudging users towards better security decisions in password creation using whitebox-based multidimensional visualisations. *Behaviour & Information Technology*, *41*(7), 1357–1380. https://doi.org/10.1080/0144929x.2021.1876167

Hausken, K. (2008). Strategic defense and attack for series and parallel reliability systems. *European Journal of Operational Research*, *186*(2), 856–881. https://doi.org/10.1016/j.ejor.2007.02.013

Hausken, K. (2015). A strategic analysis of information sharing among cyber attackers. *Journal of Information Systems and Technology Management*, *12*(2). https://doi.org/10.4301/s1807-17752015000200004

Hausken, K. (2017a). Information sharing among cyber hackers in successive attacks. *International Game Theory Review*, *19*(2), 750010.

Hausken, K. (2017b). Security investment, hacking, and information sharing between firms and between hackers. *Games*, *8*(2), 23.

He, C. Z., Frost, T., & Pinsker, R. E. (2019). The impact of reported cybersecurity breaches on firm innovation. *The Journal of Information Systems/Journal of Information Systems*, *34*(2), 187–209. https://doi.org/10.2308/isys-18-053

Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management*, *52*(3), 337–347. https://doi.org/10.1016/j.im.2014.12.006

Hovav, A., & D'Arcy, J. (2003). The impact of Denial-of-Service attack announcements on the market value of firms. *Risk Management and Insurance Review*, *6*(2), 97–121. https://doi.org/10.1046/J.1098-1616.2003.026.x

Hovav, A., & D'Arcy, J. (2005). Capital market reaction to defective IT products: The case of computer viruses. *Computers & Security*, *24*(5), 409–424. https://doi.org/10.1016/j.cose.2005.02.003

Hovav, A., & Gray, P. (2014). The ripple effect of an information security breach event: A stakeholder analysis. *Communications of the Ais*, *34*(1), 50. https://aisel.aisnet.org/cais/vol34/iss1/50/

Huang, H. H., & Wang, C. (2021). Do banks price firms' data breaches? *The Accounting Review*, *96*(3), 261–286. https://doi.org/10.2308/TAR-2018-0643

Huang, Z., Biczók, G., & Liu, M. (2024). Incentivizing secure software development: The role of liability (Waiver) and audit. *ArXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2401.08476

Iuga, N. (2016). Erola Baiting the hook: factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Science* 6(8).

Jamilov, R., Rey, H., & Tahoun, A. (2023). The anatomy of cyber risk. NBER Working Paper no. 2890.

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*(2), 85–105. https://doi.org/10.1509/jm.16.0124

Jeong, C. Y., Lee, S. Y. T., Joon, S., Lim, & Lim, J. H. (2019). Information security breaches and IT security investments: Impacts on competitors. *Information & Management*, *56*(5), 681–695. https://doi.org/10.1016/j.im.2018.11.003

Jeske, D., Coventry, L., Briggs, P., & Van Moorsel, A. (2014). *Nudging whom how: IT proficiency, impulse control and secure behavior*. Abertay University. https://rke.abertay.ac.uk/en/publications/nudging-whom-how-it-proficiency-impulse-control-and-secure-behavi

Johnson, M., Kang, M. J., & Lawson, T. (2017). Stock price reaction to data breaches. *Journal of Finance Issues*, *16*(2), 1–13. https://doi.org/10.58886/jfi.v16i2.2263

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, *46*(4), 757–780. https://doi.org/10.1111/1467-954X.00139

Junior, R. C., Becker, I., & Johnson, S. (2023). Unaware, unfunded and uneducated: A systematic review of SME cybersecurity. *ArXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2309.17186

Kamiya, S., Kang, J., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kankane, S., DiRusso, C., & Buckley, C. (2018). Can we nudge users toward better password management? *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (CHI EA '18)*. https://doi.org/10.1145/3170427.3188689

Kelley, H. W., & Warner, H. (2023). Analytical reasoning reduces internet fraud susceptibility. *Computers in Human Behavior*, *142*, 107648.

Khan, K., Khurshid, A., & Cifuentes-Faura, J. (2024). Is artificial intelligence a new battleground for cybersecurity? *Internet of Things*, *28*, 101428. https://doi.org/10.1016/j.iot.2024.101428

Kim, B. C., Chen, P., & Mukhopadhyay, T. (2011). The effect of liability and patch release on software security: The monopoly case. *Production and Operations Management*, *20*(4), 603–617. https://doi.org/10.1111/j.1937-5956.2010.01189.x

Kim, J. B., Song, B. Y., & Stratopoulos, T. (2018). Does information technology reputation affect bank loan terms? *The Accounting Review*, *93*(3), 185–211.

Kour, R., Karim, R., & Dersin, P. (2025). Modelling cybersecurity strategies with game theory and cyber kill chain. *Int J Syst Assur Eng Manag*. https://doi.org/10.1007/s13198-025-02733-4

Kovenock, D., & Roberson, B. (2018). The optimal defense of networks of targets. *Economic Inquiry*, *56*(4), 2195–2211. https://doi.org/10.1111/ecin.12565

Kude, T., Hoehle, H., & Sykes, T. A. (2017). Big data breaches and customer compensation strategies: Personality traits and social influence as antecedents of perceived compensation. *International Journal of Operations & Production Management*, *37*(1), 56–74. https://doi.org/10.1108/IJOPM-03-2015-0156

Kunreuther, H., & Heal, G. (2003). Interdependent security. *Journal of Risk and Uncertainty*, *26*(2/3), 231–249. http://www.jstor.org/stable/41755017

Kwon, J., & Johnson, M. E. (2015). The Market Effect of Healthcare Security: Do Patients Care about Data Breaches? Workshop on the Economics of Information Security. https://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_kwon.pdf

Labrecque, L. I., Markos, E., Swani, K., & Peña, P. (2021). When data security goes wrong: Examining the impact of stress, social contract violation, and data type on consumer coping responses following a data breach. *Journal of Business Research*, *135*, 559–571. https://doi.org/10.1016/j.jbusres.2021.06.054

Lam, W. M. W. (2016). Attack-prevention and damage-control investments in cybersecurity. *Information Economics and Policy*, *37*, 42–51. https://doi.org/10.1016/j.infoecopol.2016.10.003

Lam, W. M. W., & Seifert, J. (2023). Regulating data privacy and cybersecurity. *The Journal of Industrial Economics*, *71*(1), 143–175. https://doi.org/10.1111/joie.12316

Lee, C. H., Geng, X., & Raghunathan, S. (2016). Mandatory standards and organizational information security. *Information Systems Research*, *27*(1), 70–86. https://doi.org/10.1287/isre.2015.0607

Lemnitzer, J. M. (2021). Why cybersecurity insurance should be regulated and compulsory. *Journal of Cyber Policy*, *6*(2), 118–136. https://doi.org/10.1080/23738871.2021.1880609

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. https://doi.org/10.1007/s10898-017-0585-y

Lulandala, E. E. (2020). Facebook data breach: A systematic review of its consequences on consumers' behaviour towards advertising. In P. K. Kapur, O. Singh, S. K. Khatri, & A. K. Verma (Eds.), *Strategic system assurance and business analytics. Asset analytics*. Springer. https://doi.org/10.1007/978-981-15-3647-2_5

Madarie, R. (2017). Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers. *International Journal of Cyber Criminology*, 11(1).

Maillart, T., Zhao, M., Grossklags, J., & Chuang, J. (2017). Given enough eyeballs, all Bugs are shallow? Revisiting Eric Raymond with bug bounty programs. *Journal of Cybersecurity*, *3*(2), 81–90. https://doi.org/10.1093/cybsec/tyx008

Makridis, C. A. (2021). Corrigendum to: Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab022

Malhotra, A., & Malhotra, C. K. (2011). Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research*, *14*(1), 44–59. https://doi.org/10.1177/1094670510383409

Markos, E., Peña, P., Labrecque, L. I., & Swani, K. (2023). Are data breaches the new norm? Exploring data breach trends, consumer sentiment, and responses to security invasions. *The Journal of Consumer Affairs*, *57*(3), 1089–1119. https://doi.org/10.1111/joca.12554

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, *24*, 35–61. https://doi.org/10.1016/j.cosrev.2017.01.001

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36–58. http://www.jstor.org/stable/44879034

Matheson (2019). The Insurability of GDPR fines - Nov. 2019. Available at: https://www.matheson.com/insights/detail/the-insurability-of--gdpr-fines

Maurushat, A., & Nguyen, K. (2022). The legal obligation to provide timely security patching and automatic updates. *International Cybersecurity Law Review*, *3*(2), 437–465. https://doi.org/10.1365/s43439-022-00059-6

Miller, L. (2019). Cyber insurance: An incentive alignment solution to corporate Cyber-Insecurity. *Journal of Law & Cyber Warfare*, *7*(2), 147–182. https://www.jstor.org/stable/26777974

Mitra, A., Mohanty, S., & Kougianos, E. (2024). The world of generative AI: Deepfakes and large Language models. *ArXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2402.04373

Mookerjee, V., Mookerjee, R., Bensoussan, A., & Yue, W. T. (2011). When hackers talk: Managing information security under variable attack rates and knowledge dissemination. *Information Systems Research*, *22*(3), 606–623. https://doi.org/10.1287/isre.1100.0341

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, *3*(3–4), 103–117. https://doi.org/10.1016/j.ijcip.2010.10.002

Morgan Stanley. (2024). *AI and cybersecurity: A new era | Morgan Stanley*. :text=,review%20your%20current%20cybersecurity%20protection. https://www.morganstanley.com/articles/ai-cybersecurity-new-era#:~

Morgner, P., Mai, C., Koschate-Fischer, N., Freiling, F., & Benenson, Z. (2020). Security update labels: Establishing economic incentives for security patching of IoT consumer products. *2020 IEEE Symposium on Security and Privacy (SP)*. https://doi.org/10.1109/sp40000.2020.00021

Morse, E. A., Raval, V., & Wingender, J. R. (2011). Market price effects of data security breaches. *Information Security Journal: A Global Perspective*, *20*(6), 263–273. https://doi.org/10.1080/19393555.2011.611860

Muzatko, S., & Bansal, G. (2023). It pays to be forthcoming: Timing of data breach announcement, trust violation, and trust restoration. *Internet Research*. https://doi.org/10.1108/INTR-12-2021-0939

Nagurney, A., & Nagurney, L. S. (2015). A game theory model of cybersecurity investments with information asymmetry. *Netnomics*, *16*(1–2), 127–148. https://doi.org/10.1007/s11066-015-9094-7

Nelson, R. R., & Winter, S. G. (1985). *An evolutionary theory of economic change*. Harvard University Press.

Nofer, M., Hinz, O., Muntermann, J., & Roßnagel, H. (2014). The economic impact of privacy violations and security breaches. 6(6), 339–348. https://doi.org/10.1007/s12599-014-0351-3

OECD (2017). Enhancing the role of insurance in cyber risk management. In OECD eBooks. https://doi.org/10.1787/9789264282148-en

Osei-Bryson, K. M., Ko, M., & Zafar, H. (2012). Financial impact of information security breaches on breached firms and their Non-Breached competitors. *Information Resources Management Journal*, *25*(1), 21–37. https://doi.org/10.4018/irmj.2012010102

Patterson, A. (2020). The ongoing issue of cyber insecurity: Why cyber insurance should be mandatory for consumer companies. *Fla St UL Rev*, *48*, 841.

Peer, E., Egelman, S., Harbach, M., Malkin, N., Mathur, A., & Frik, A. (2019). Nudge me right: Personalizing online nudges to people's Decision-Making styles. *Social Science Research Network*. https://doi.org/10.2139/ssrn.3324907

Petrosyan, A. (2023). *Global cybercrime estimated cost 2028*. Statista. https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

Piccotti, L. R., & Wang, H. (2022). Informed trading in the options market surrounding data breaches. *Global Finance Journal*, 100774. https://doi.org/10.1016/j.gfj.2022.100774

Png, I. P. L., & Wang, Q. H. (2009). Information security: Facilitating user precautions Vis-à-Vis enforcement against attackers. *Journal of Management Information Systems*, *26*(2), 97–121. https://doi.org/10.2753/MIS0742-1222260205

Pym, D., Swierzbinski, J., & Williams, J. (2013). *The need for public policy interventions in information security* (pp. 1–23). University of Aberdeen. http://hdl.handle.net/2164/2966

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. https://doi.org/10.1007/s10878-019-00446-6

Ransbotham, N., Mitra, N., & Ramsey, N. (2012). Are markets for vulnerabilities effective? *Management Information Systems Quarterly*, *36*(1), 43. https://doi.org/10.2307/41410405

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft. *Journal of Policy Analysis and Management*, *30*(2), 256–286. https://doi.org/10.1002/pam.20567

Rosati, P., Cummins, M., Deeney, P., Gogolin, F., Van Der Werff, L., & Lynn, T. (2017). The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *International Review of Financial Analysis (Online)/International Review of Financial Analysis*, *49*, 146–154. https://doi.org/10.1016/j.irfa.2017.01.001

Sager, I., & Green, J. (2002). *The best way to make software secure: Liability* (Vol. 18March, p. 61). Business Week.

Sai, S., Yashvardhan, U., Chamola, V., & Sikdar, B. (2024). Generative ai for cyber security: Analyzing the potential of chatgpt, dall-e and other models for enhancing the security space. IEEE access.

Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. *Information & Management*, *59*(4), 103638. https://doi.org/10.1016/j.im.2022.103638

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*(2), 314–341. https://doi.org/10.1080/07421222.2015.1063315

Shackelford, S., Boustead, A., & Makridis, C. A. (2022). Defining reasonable cybersecurity: evidence from the states. *Yale Journal of Law and Technology*, *25*. https://yjolt.org/sites/default/files/shackelford_scott_et_al._-_reasonable_cybersecurity.86.pdf

Sharma, K., Zhan, X., Nah, F. F., Siau, K., & Cheng, M. X. (2021). Impact of digital nudging on information security behavior: An experimental study on framing And priming in cybersecurity. *Organizational Cybersecurity Journal*, *1*(1), 69–91. https://doi.org/10.1108/ocj-03-2021-0009

Sheng, H., & Kumaraguru, Cranor, D. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In: Proceedings of the SIGCHI conference on human factors in computing systems. ACM, New York, 373–382.

Shevchenko, P. V., Jang, J., Malavasi, M., Peters, G. W., Sofronov, G., & Trück, S. (2023). The nature of losses from cyber-related events: Risk categories and business sectors. *Journal of Cybersecurity*, *9*(1), tyac016. https://doi.org/10.1093/cybsec/tyac016

Slepchuk, A. N., Milne, G. R., & Swani, K. (2021). Overcoming privacy concerns in consumers' use of health information technologies: A justice framework. *Journal of Business Research*. https://doi.org/10.1016/j.jbusres.2021.11.073

Smith, I. (2023). Is state intervention needed for cyber insurance? Financial Times. Retrieved September 26, 2024, from https://www.ft.com/content/e5fa921b-8929-442b-8ab5-261229d0802d

Smith, T., Tadesse, A. F., & Vincent, N. E. (2021). The impact of CIO characteristics on data breaches. *International Journal of Accounting Information Systems*, *43*, 100532. https://doi.org/10.1016/j.accinf.2021.100532

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market. *Computers & Security*, *58*, 216–229. https://doi.org/10.1016/j.cose.2015.12.006

Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering*, *33*(8), 544–557. https://doi.org/10.1109/tse.2007.70712

Thomas, D. R., & Beresford, A. R. (2016). *Incentivising software updates*. Paper presented at Internet of Things Software Update Workshop (IoTSU), Dublin, Ireland. https://doi.org/10.17863/CAM.7788

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, *76*, 101795. https://doi.org/10.1016/j.irfa.2021.101795

Truong, T. C., Zelinka, I., Plucar, J., Čandík, M., & Šulc, V. (2020). Artificial intelligence and cybersecurity: Past, presence, and future. *Artificial intelligence and evolutionary computations in engineering systems* (pp. 351–363). Springer Singapore.

Turjeman, D., & Feinberg, F. M. (2024). When the data are out: measuring behavioral changes following a data breach. *Marketing Science*, 43(2), 440–461. https://doi.org/10.1287/mksc.2019.0208.

Tweneboah-Koduah, S., Atsu, F., & Prasad, R. (2020). Reaction of stock volatility to data breach: An event study. *Journal of Cyber Security and Mobility*, 1–19. https://doi.org/10.13052/jcsm2245-1439.931

Uddin, M., Irshad, M. S., Kandhro, I. A., Alanazi, F., Ahmed, F., Maaz, M., Hussain, S., & Ullah, S. S. (2025). Generative AI revolution in cybersecurity: A comprehensive review of threat intelligence and operations. *Artificial Intelligence Review*, *58*(8). https://doi.org/10.1007/s10462-025-11219-5

Varian, H. R. (2000). *Managing online security risks* (p. 1). New York Times.

Varian, H. R. (2004). System reliability and free riding. In J. J. Camp, & S. Lewis (Eds.), *Economics of information security* (Vol. 12). Springer. Advances in Information Securityhttps://doi.org/10.1007/1-4020-8090-5_1

Vasek, M., Wadleigh, J., & Moore, T. (2016). Hacking is not random: A case-control study of webserver-compromise risk. *IEEE Transactions on Dependable and Secure Computing/IEEE Transactions on Dependable and Secure Computing*, *13*(2), 206–219. https://doi.org/10.1109/tdsc.2015.2427847

Vergara Cobos, E., & Selcen, C. (2024). *A review of the economic costs of cyber incidents*. World Bank.

Verizon (2024). Data Breach Investigations Report. In https://www.verizon.com. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

Wang, Q., Ngai, E. W. T., Pienta, D., & Thatcher, J. B. (2023). Information technology innovativeness and Data-Breach risk: A longitudinal study. *Journal of Management Information Systems*, *40*(4), 1139–1170. https://doi.org/10.1080/07421222.2023.2267319

Watson, R., & Bergman, R. (2024). How can cybersecurity transform to accelerate value from AI? https://www.ey.com. Retrieved June 14, 2025, from https://www.ey.com/en_us/insights/consulting/transform-cybersecurity-to-accelerate-value-from-ai

Woods, D. W., & Moore, T. (2020). Does insurance have a future in governing cybersecurity? *IEEE Security & Privacy*, *18*(1), 21–27. https://doi.org/10.1109/msec.2019.2935702

Woods, D., & Simpson, A. (2017). Policy measures and cyber insurance: A framework. *Journal of Cyber Policy*, *2*(2), 209–226. https://doi.org/10.1080/23738871.2017.1360927

World Economic Forum (2024). *Global Cybersecurity Outlook 2024*. (2024). https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

Wu, Y., Duan, J., Dai, T., & Cheng, D. (2020). Managing security outsourcing in the presence of strategic hackers. *Decision Analysis*, *17*(3), 235–259. https://doi.org/10.1287/deca.2019.0406

Wu, X., Wu, Y., Li, Q., & Dai, T. (2023). How to React to hacker types and asset types in security decision-making. *Expert Systems with Applications*, *231*, 120654. https://doi.org/10.1016/j.eswa.2023.120654

Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, *26*(1), 60–77. https://doi.org/10.1057/jit.2010.4

Yin, T., Sarabi, A., & Liu, M. (2023). Deterrence, backup, or insurance: Game-Theoretic modeling of ransomware. *Games*, *14*(2), 20. https://doi.org/10.3390/g14020020

Zafar, H., Ko, M., & Osei-Bryson, K. (2016). The value of the CIO in the top management team on performance in the case of information security breaches. *Information Systems Frontiers*, *18*(6), 1205–1215. https://doi.org/10.1007/s10796-015-9562-5

Zhao, M., Grossklags, J., & Liu, P. (2015). An Empirical Study of Web Vulnerability Discovery Ecosystems. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15). Association for Computing Machinery, New York, NY, USA, 1105–1117. https://doi.org/10.1145/2810103.2813704

Zimmermann, V., & Renaud, K. (2021). The nudge puzzle. *ACM Transactions on Computer-human Interaction*, *28*(1), 1–45. https://doi.org/10.1145/3429888

Zou, Y., Le, K., Mayer, P., Acquisti, A., Aviv, A. J., & Schaub, F. (2024). *Nudging Users to Change Breached Passwords Using the Protection Motivation Theory* (arXiv:2405.15308). arXiv. http://arxiv.org/abs/2405.15

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Laura Abrardi[1] · Stefano Comino[2] · Sasha Grassini[1]

✉ Laura Abrardi
laura.abrardi@polito.it

Stefano Comino
stefano.comino@uniud.it

Sasha Grassini
sasha.grassini@polito.it

[1] Department of Management, Politecnico di Torino, Corso Duca degli Abruzzi, 24, Turin 10129, Italy

[2] Department of Economics and Statistics, Università degli Studi di Udine, Via Tomadini, 30/A, 33100 Udine, Italy