A Review of the Economic Costs of Cyber Incidents

Estefania Vergara Cobos[1], Selcen Cakir[2] [3]

[**Attribution—**Please cite this work as follows: Vergara Cobos, Estefania; and Cakir, Selcen. 2024. A Review of the Economic Costs of Cyber Incidents. Washington, DC: World Bank.] [4]

Abstract

Given the rapid digitization of societies and the increase in costly and sophisticated cyber incidents, there is a rising need to prioritize cybersecurity in the investment agendas of economic actors, especially, governments and firms. However, a major bottleneck in mainstreaming cybersecurity investments is the unclarity in the returns and the unidentified link between cyber incidents and economic performance.

This literature survey brings together empirical studies on the direct and indirect costs of cyber incidents, highlighting issues in the study of risk-based approaches based on current estimates that could lead to misinformed decisions. First, this survey identifies the vast variety of unfounded estimates of the cost of cyber incidents. Second, the analysis dives into the difficulty of assessing the full spectrum of costs due to the existence of nonnegligible indirect costs.

This article argues that to accurately protect cyberspace, policymakers and stakeholders should aim to understand the full spectrum of economic costs of cyber incidents by promoting research through data collection efforts.

Keywords: Cybersecurity incidents, economic loss, defense, direct and indirect costs.

JEL codes: O33, O38, O39, L96, M15

[1] Economist, Infrastructure Chief Economist Office, World Bank (evergaracobos@worldbank.org).

[2] Assistant Professor of Economics at Bogazici University (selcen.cakir@boun.edu.tr).

[3] This paper is a product of the Chief Economist Office for the Infrastructure Vice-Presidency of the World Bank. This research was funded by the World Bank Cybersecurity Multi-Donor Trust Fund as part of a larger effort to study the Economics of Cybersecurity. The authors wish to thank Stephane Straub, Christine Zhenwei Qiang, and Casey Torgusson for their comments and support, and country donors of the World Bank Cybersecurity Multi-Donor Trust Fund for funding this work.

1. Introduction

Given the rapid digital transformation of nations, it is increasingly important to understand the economic impact of cyber incidents to ensure adequate protection of cyberspace. Cyber incidents—disruptions caused by malicious network or system breaches[5] —pose a considerable threat to economic, social, and political structures of societies. This paper presents a comprehensive review of the existing research on costs incurred from cyber incidents to show the wide range of economic costs and potential risks linked to cyber incidents, differentiating between direct costs—tangible, immediate economic losses such as ransom payments—and indirect costs— such as those from cascading effects and long-term reputational damages.

When considering investments in cybersecurity, both public and private sectors are challenged by the difficulty of assessing the net benefits due to the inherent complexity of determining the likelihood and potential value at risk of breaches (Gordon et al., 2020). Our study aims to consolidate various cost estimates from empirical literature to enhance the understanding of the types of losses incurred from cyber incidents, the methodologies used for loss estimation, and the available data sources on cybersecurity incidents. Prior studies and reports (PwC, 2018; Romanosky et al., 2019) have stressed the importance of closing this knowledge gap, indicating that a deeper understanding of the economic costs of cyber incidents is crucial for more effective decision-making and policy formation (U.S. CISA, 2021).

This paper synthesizes over 50 academic papers and various "well-cited" industry reports, showing that while the direct costs of cyber incidents could represent an important share of countries' economies, the indirect costs could be at least as important. Especially, since cyber incidents have the capacity to pose risks to the macroeconomic stability of nations, such as systemic disruptions across financial markets (Corbet and Gurdgiev, 2019; Jamilov et al., 2021) and considerable losses in the stocks markets (Amir et al., 2018; Akey et al., 2021; Kamiya et al., 2021; Lending et al., 2018; Piccotti and Wang, 2022; Lin et al., 2020; Tosun, 2021).

This review has two major policy recommendations. First, we highlight the scarcity of reliable data and the lack of standardized cybersecurity definitions as critical barriers to developing robust economic cost assessments and effective policies. Therefore, we advocate for enhanced international cooperation to monitor cyber incidents on a global scale. Second, we recognize the role of indirect costs from cyber incidents and cybersecurity market failures to advocate for a more active role from governments but under the understanding that cybersecurity is a shared responsibility amongst all economic actors.

This paper is organized as follows. The next section discusses rough estimates of the direct costs of cyber incidents, compiled mainly from industry reports. Then, Section 3 discusses the recent literature on the indirect costs of cyber incidents such as stock markets effects, spillover effects, reputational damages, systemic risks, costs associated with delayed announcement, the response costs, and the costs associated with cyber risks. Section 4 presents the main challenges for having more accurate and reliable estimates on the economic costs of cyber incidents. Finally, Section 5 summarizes and engages in a discussion of policy implications.

2. The direct costs of cyber incidents

Direct costs associated with cyber incidents encompass the tangible financial losses, damages, and hardships endured by victims following such events. These include, but are not limited to, the illicit financial gains accrued by cybercriminals (Anderson et al., 2013). This section compiles data from fifteen prominent industry reports published between 2017 and 2023 to construct a clearer picture of the direct costs attributable

[5]A cyber incident is an event or the end result of any single unauthorized effort taken using an information system (e.g., computer technology) or network that resulted in an actual or potentially nationally relevant adverse effect on any of the three layers that constitute cyberspace, including information systems, networks, and/or the information residing therein (Harry et al., 2023, NIST).

to cybersecurity breaches. Through this examination, we seek to shed light on the escalating cost trajectory of cyber incidents across various regions and sectors. However, it is important to note a significant limitation: these industry reports often lack transparency in their estimation methodologies and data sourcing, which hampers our ability to substantiate their accuracy.

Table 1 presents the great variety of aggregated estimates of the annual global costs of cyber incidents reported by some of the most cited industry reports. While these numbers have been highly quoted by the cybersecurity community, the validity of the methodologies used cannot be assess.

Table 1: Aggregated estimates of the annual global cost of all cybersecurity incidents

Report and Year of Publication	**Methodology**	**Limitation**	**Aggregated Global Annual Cost Estimate (USD Billions)**	**% of Global GDP**
IC3 (2017) *	Unavailable.	Data source is the complaints received by the IC3, which are a fraction of the incidents in the U.S.	1.42	0.0018%
Norton (2017)	Online survey with 21,539 individuals ages 18+ across 20 countries	Captures only the losses of consumers	172	0.21%
McAfee and CISS (2018)	Compiles from literature the direct and indirect loss estimates for many countries and aggregates them with an unavailable methodology.	Data is subject to measurement error	522.5	0.6%
eSentire & Cybersecurity Ventures (2019)	Unavailable	Estimates are based on historical cybercrime rates.	6,000	6.9%
IC3 (2019) *	Unavailable	Data source is the complaints received by the IC3, which are a fraction of the incidents in the U.S.	2.71	0.003%
IC3 (2020)*	Unavailable	Data source is the complaints received by the IC3, which are a fraction of the incidents in the U.S.	3.50	0.004%
European Commission (2021)*	Unavailable	Data source is not available.	6,070	7.1%
eSentire & Cybersecurity Ventures (2022)	.Unavailable	Estimates are based on historical cybercrime rates.	8,000 (2023 projection)	8%
eSentire & Cybersecurity Ventures (2022)	.Unavailable	Estimates are based on historical cybercrime rates.	10,500 (2025 projection)	9.1%

Note: These aggregate estimates do not differentiate the severity or type of cybersecurity incident. The methodologies used to estimate these findings have not been validated by the authors of this chapter. *Reports included from the same period but not necessarily from industry stakeholders have been added for comparative purposes. The source for global nominal GDP (in USD) is the IMF.

Despite the dispersity of cost estimates, these industry reports show that the overall global costs have been steadily increasing across various sectors, including credit card theft, ransomware attacks, and security breaches in large enterprises, as well as small and medium-sized businesses. Industry projections for the next few years place crypto crime and ransomware attacks at the top of the fastest growing cyber incidents, with worldwide cost estimates projected to reach USD 30 billion per year by 2025 and USD 265 billion per year by 2031, respectively (eSentire & Cybersecurity Ventures, 2022).[6] Similarly, data breaches were expected to represent higher costs and reach an all-time high of USD 4.35 million (IBM, 2022) per breach.

Due to limited resources, inadequate infrastructure, and limited access to skilled cybersecurity professionals, developing countries often face distinct difficulties in implementing effective cybersecurity capacity building and commitments (ITU, 2021). For example, in Africa, the financial consequences of cyber incidents could be substantial, as more than 90% of African businesses operate without proper protocols in place (CGTN, 2020). Moreover, the rapid digitization across the continent gives rise to new and costlier types of cyber threats, increasing the danger to the stability and functioning of the economy (Interpol, 2021; Africa Center for Strategic Studies, 2021). Although up-to-date cost estimates of cyber incidents in Africa are limited, figures from 2016 indicate that cybercrime costs the Kenyan economy USD 36 million per year or about 0.05% of the country's GDP, the South African economy USD 573 million or 0.17% of GDP, and the Nigerian economy USD 500 million or 0.12% of its annual GDP (Interpol, 2016). However, research done by Kenyan IT cybersecurity firm Serianu in 2021 revealed that cybercrime has reduced Africa's GDP by more than 10%, amounting to an estimated loss of USD 4.12 billion only in that year (Phys.org, 2021).[7]

Like for Africa, country-level cost indicators for the other regions are rare, and even when they are available, the data usually comes from developed countries with robust policies to accurately monitor cybersecurity breaches over time. For example, according to the UK Cabinet Office, in 2011, the UK government estimated that the costs of cybercrime was USD 33.67 billion or about 1.3% of the country's GDP, with the largest share posed to businesses—about 77.78%. Grant Thornton (2021) shows that in 2014, the total cost of cybercrime in Ireland was USD 695.5 million, and then, in 2020, it increased dramatically to USD 10.5 billion, or 2.5% of the country's GDP. A similar number is drawn for Brazil, where the demand for cyber risk insurance has soared in the last few years as the costs of cybercrime in the country were estimated to be at around USD 8 billion in 2015, or about 0.4% of the countries' GDP.[8] (See Appendix II for a detailed compilation of the main estimations on the economic costs of cybersecurity incidents from industry published in the 2017-2023 period).

3. The indirect costs of cyber incidents

Indirect costs from cyber incidents are difficult to quantify and are often ignored; although, they can have important long-term impacts on the economy (Campbell et al., 2003; Cybereason, 2022). Indeed, indirect costs can be at least as important as direct costs because of the various after-incident costs that are intertwined with the continuation of activities and the externalities that are generated on a structural level. For example, Kamiya et al. (2021) focus on 75 firms with first-time cyberattacks, and find that the indirect costs (e.g., investigation and remediation costs, legal penalties, and regulatory penalties) are much lower (USD 1.2 billion) than the total shareholder wealth losses (USD 104 billion) following a data breach announcement. Similarly, according to the

[6] Moreover, IBM's *Cost of a Data Breach* report (2022) indicates that ransomware breach costs of 2022 have slightly decreased compared to the year before, from USD 4.62 million to USD 4.54 million. However, the occurrence of ransomware breaches has increased, with 11% reported in the 2022 study, up from 7.8% in the 2021 report.

[7] Growing reliance on digital systems and infrastructure exposes countries to more significant risks, potentially leading to disruptions in essential services such as healthcare, finance, and transportation—some of the key sectors that often make the headlines with significant economic losses resulting from cybersecurity incidents. Furthermore, the expanding scope of incidents can strain law enforcement and technological and human resources, making it difficult for governments to respond effectively to emerging threats.

[8] https://securityintelligence.com/the-true-cost-of-cybercrime-in-brazil/

Accenture and Ponemon Institute (2019), firms face the risk of losing an estimated USD 5.2 trillion in value creation opportunities from the digital economy due to cyberattacks until 2024, which is nearly equivalent to the combined economies of France, Italy, and Spain.

This literature review has identified the most cited academic studies covering indirect costs, which are mainly related to the study of stock market reactions and reputational damages, production chain disruptions, spillover effects and systematic risks posed by cyber incidents, costs associated with delayed announcement, response costs, and the costs associated with cyber risk.

3.1 Stock market reactions to cyber incidents and reputational effects

Much research focuses on the effects of cyber breach announcements on a firm's stock market value. Early empirical studies find either null or small effects (Hovav and D'Arcy, 2003; Campbell et al., 2003; Acquisti et al., 2006; Kannan et al., 2007; Wang et al., 2013). For example, using an event study methodology and data on cyber incidents between 1996 and 2000, Campbell et al. (2003) find limited evidence that cyber breaches reported in newspapers influence publicly traded US corporations, pointing at significant effects only from breaches involving unauthorized access to confidential data. In contrast, studies using more recent data quantify large and significant negative stock market effects from breach announcements (Amir et al., 2018; Akey et al., 2021; Kamiya et al., 2021; Lending et al., 2018; Piccotti and Wang, 2022; Lin et al., 2020; Tosun, 2021). Using data from 2005-2016, Iyer et al. (2020) show that the value of corporate bonds also decreases following a breach announcement, with bondholders losing approximately 2% of wealth within one-month after the announcement.

Literature indicates that there are heterogeneous stock market reactions to a cyber breach announcement depending on the type of attack. For example, Goldstein et al. (2011) use a dataset covering all public operational failure events in the U.S., including cybersecurity-related ones, to find that the market value of firms that have function-related failures drop more (1.48%) compared to firms that have data-related failures (0.75%). Garg et al. (2003) find that while all types of IT security breaches yield negative market returns, the market reacts most to credit card information theft (9-15%) and DoS incidents (1-4%). Akey et al. (2021) show that firms' value declines more after data breaches involving customer records as opposed to those involving employee records. Finally, Piccotti and Wang (2022) show that among four types of breaches (i) hacking or malware, ii) paper documents that are lost, discarded or stolen, iii) lost, discarded, or stolen portable devices, and iv) unknown), only breaches that involve hacking of portable devices have a significant negative effect on stock market return.

In addition to causing stock market losses, cyber breach announcements may also affect a firm's value by damaging its brand value. For example, using firm-level data between 2002 and 2018, Makridis (2018) find that large data breaches are associated with a loss of 5-9% reputational intangible capital by looking at the change in a firm's brand power ranking.

To formalize the empirical findings on stock market losses of cyber breach announcements, Kamiya et al. (2021) build a model of the optimal cybersecurity risk for a firm. In their model, a firm invests in risk mitigation to manage the stakeholders' assessment of the firm's loss distribution from potential risks. When a cyber breach occurs, it can alter stakeholders' perceptions, prompting them to adjust their investments based on the new, often increased, perception of risk. This shift can lead to substantial reputational and financial damages for the company, especially if the updated perception of risk is significantly negative. The observed decrease in stock prices following announcements of cyber breaches is therefore seen as a reflection of diminished trust and confidence in the company from consumers and investors.

Table 2 reviews this literature, showing that studies on reputational and stock market damages are concentrated in the United States, thanks to the availability of the open-source U.S. Privacy Rights Clearing House (PRC) database on disclosed cyber breaches.

Table 2: Summary of the stock market effects of cybersecurity incidents

Paper	Main finding	Cybersecurity breach/risk data set	Sample	Time coverage
Positive or neutral effects				
Garg (2020)	Firms hold more cash after having a cyberattack. Their suppliers and unaffected peer firms also increase their cash holdings.	PRC	United States	2005-2017
Makridis (2021)	Large (small) data breaches are associated with a loss (gain) of 5-9% (26-29%) reputational intangible capital or firm's brand value.	PRC	United States	2002-2018
Bose and Leung (2013)	The announcement of employing identity theft counter measures is associated with a 0.63% increase in a firm's market value.	Construct own dataset from news databases	United States	1995-2012
Akey et al. (2021)	Firms compensate for the erosion of their reputation following a data breach by investing 0.4-0.5 standard deviations more in corporate social responsibility.	PRC	United States	2005-2016
Kannan et al. (2007)	There are no significant negative market returns to information security breach announcements.	Construct own dataset from news databases	United States	1997-2003
Negative effects				
Wang et al. (2022)	Prior to breach announcements, attacked firms have 6.8% higher Daily Cost of Borrow Score (DCBS), 0.27% higher loan fees, and 0.3% lower rebate fees. The abnormal level of trading activity suggests that short sellers exploit insider knowledge of breaches.	PRC	United States	2005-2018
Amir et al. (2018)	Managers disclose information on cyberattacks when investors already suspect a high probability of an attack. Withheld (disclosed) cyberattacks are associated with a 2.6% (0.7%) decrease in equity values.	1. Audit Analytics 2. VCDB VERIS	United States	2010-2015
Goldstein et al. (2011)	The market value of firms that have function-related failures drop more (1.48%) compared to firms that have data-related events (0.75%).	FIRST	United States	1985-2009
Makridis (2021)	Large (small) data breaches are associated with a loss (gain) of 5-9% (26-29%) reputational intangible capital.	PRC	United States	2002-2018
Iyer et al. (2020)	Following a data breach announcement, corporate bond holders have 2% negative returns in a month.	PRC	United States	2005-2016
Akey et al. (2021)	Firms that announce a breach have 1.5–1.9% reduction in cumulative abnormal returns in 30 days. Firms with higher pre-event investment in corporate social responsibility do not lose as much.	PRC	United States	2005-2016
Kamiya et al. (2021)	Disclosure of a cyberattack significantly reduces shareholder wealth and sales growth.	PRC	United States	2005-2017

	Shareholder wealth decreases by 1.09% within 3 days after an attack announcement.			
Garg et al. (2003)	All types of IT security breaches yield negative market returns. The market reacts especially to credit card information theft (9-15%) and DoS incidents (1-4 %).	Construct own dataset from news databases	United States	1996-2002
Hovav and D'Arcy (2003)	Following a DoS attack, companies that rely on their web sites for their business operations have negative stock market returns while non-internet specific companies do not experience any reactions.	Construct own dataset from news databases	United States	1998-2002
Lending et al. (2018)	Firms have –1.4% reduction in returns within 3 days of a breach announcement. Moreover, attacked firms experience 3.5% reduction in one-year buy-and-hold abnormal returns. Firms with larger boards and boards with less financial expertise are more likely to be a target while socially responsible firms are less likely to be a target. Firms that improve their governance and social capital following a breach reduce the likelihood of a further breach by 5.03% to 6.78%.	PRC	United States	2004-2012
Piccotti and Wang (2022)	Transactions in the options market indicate that hackers (insiders) initiate informed trading 12 (4) months prior to data breach announcements. On average, cumulative abnormal returns of breached firms decrease by 0.46% following a breach within 5 days.	PRC	United States	2005-2018
Lin et al. (2020)	Insiders save an average of USD 35,000 due to short selling. Following a data breach announcement, stock prices decrease by 1.18% in 3-day window, 1.44% in 5-day window, 1.26% in 21-day window, and 1.44% in 41-day window.	PRC	United States	2011-2016
Campbell et al. (2003)	There is limited evidence of an overall negative effect of information security breaches on the stock market value of firms. Cumulative abnormal returns of firms decrease by 1.8% following a breach announcement involving unauthorized access to confidential data.	Construct own dataset from news databases	United States	1996-2000
Tosun (2021)	A cyberattack has significant negative effect on a firm's stock market value and trading in the short term. Although a cyberattack has no long-run effects on a firm's market value, an impacted firm changes its policies in the long run by investing more in R&D and the CEO.	PRC	United States	2004-2019
Cavusoglu (2004)	On average, firms lose 2.1% of their market value within two days of the announcement of a cybersecurity breach.	Construct own dataset from news databases	United States	1996-2001

Wang et al. (2013)	Firms that disclose risk-mitigating information in their financial reports are less likely to have a security incident. Once a breach occurs, the market punishes the firms that take precautionary action less severely.	Construct own dataset from news databases	United States	1997-2008
Acquisti et al. (2006)	There is a significantly negative but short-lived stock market effect to privacy breach events.	Construct own dataset from news databases	United States	1999-2006
Makridis (2021)	Large (small) data breaches are associated with a loss (gain) of 5-9% (26-29%) reputational intangible capital.[9]	PRC	United States	2002-2018
Wang et al. (2022)	Abnormal levels of trading activity before data breach announcements indicate that sellers exploit prior knowledge of data breaches.	PRC	United States	2005-2018
Piccotti and Wang (2022)	Transactions in the options market indicate that hackers (insiders) initiate informed trading 12 (4) months prior to data breach announcements.	PRC	United States	2005-2018

Source: Authors' own elaboration.

3.2 Supply chain, systemic risks, and spillover effects

Cyber incidents can cause firms to lose valuable information and incur large reputational and legal costs. Yet, cyberattacks can also distort a firm's operations and production of goods and services in the short and long term, in which case the entire supply chain, the customer relationships, and even the production of peer firms could be affected. For example, Kamiya et al. (2021) investigate the attacked firms' sales growth in the post-attack period compared to similar firms that were not hit by an attack and find that sales growth declines significantly for 3 years after the attack. On the other hand, Crosignani et al. (2023) study the effects of the NotPetya attack of Russian military intelligence to Ukrainian organizations in June 2017 and show that the attack propagated from the directly hit firms to the productive capacities of their customers, causing a four-fold amplification of the initial drop in profits. Mainly, the authors estimate that NotPetya caused at least USD 7.3 billion losses by the affected customers, an amount four times larger than the losses reported by the firms directly hit by the cyberattack.

Cyber incidents can also cause contagion effects, especially in the financial sector. Kotidis and Schreft (2022) study the effects of a multi-day cyberattack on a U.S. technology service provider (TSP) and find that the cyberattack impaired the ability of TSP's customers (banks) to send payments, which left other banks with fewer resources and at risk of not being able to send their own payments. The authors show that the precautionary actions taken by the secondarily affected banks prevented the crisis from having a third-round effect. Similarly, Kamiya et al. (2021) show that the disclosure of an attack adversely affects firms operating in the same industry as the target firm, which is consistent with the authors' theory that the disclosure of a cyberattack is especially harmful when it alters the investors' perception of the risk distribution in the industry. Similarly, Jamilov et al. (2021) show that firm-level risk can be a source of systematic risk in financial markets. On the other hand, Corbet and Gurdgiev (2019) review the literature and find evidence of systemic contagion from the equity price volatility of the impacted firms to the exchange which lists the firm, and to other exchanges that list the exchange. They identify four channels of contagion through which cyber risk can be

[9] The paper claims that breaches increase brand power and familiarity-as in the saying "there is no such thing as bad advertisement."

transmitted across firms and markets, i) technology-related channels, ii) correlated risks channels, iii) network contagion, and iv) complex environments of operations.

Table 3: Summary of the literature on supply chain effects, systemic risk, and spillover effects of cyber incidents

Paper	Main finding	Cybersecurity breach/risk data set	Sample	Time coverage
Negative effects				
Crosignani et al. (2023)	Worldwide suppliers and customers of firms whose operations were halted due to the NotPetya cyberattack incurred large losses. As a result, directly-hit firms had long-lasting reputation losses.	Compiled by the authors	Ukrainian firms hit by NotPetya & their worldwide customers and suppliers	2017-2018
Kamiya et al. (2021)	Disclosure of a cyberattack reduces the sales growth of large firms, especially those in the retail industry, for 3 years.	PRC	United States	2005-2017
Kotidis and Schreft (2022)	A multi-day cyberattack on a technology service provider (TSP) impaired customers' ability to send payments, which spilled over to the banks that did not use the TSP and left them with fewer reserves.	Single event, proprietary dataset	United States	N/A
Corbet and Gurdgiev (2019)	The stock price volatility of a large firm following a data breach announcement creates volatility in both domestic and global markets, especially after 2014.	Construct own dataset from news databases	United States	2005-2015
Garg (2020)	Firms hold more cash after having a cyberattack. Their suppliers and unaffected peer firms also increase their cash holdings.	PRC	United States	2005-2017
Jamilov et al. (2021)	Firm-level cyber risk can be a source of systematic risk in financial markets.	Textual analysis of quarterly earnings announcement & Q&A sessions	85 countries	2002-2021

Source: Authors' own elaboration.

3.4 Costs arising from delayed announcement

Cyber incidents are typically announced with delay. For example, IBM (2022) estimates that the average time to identify and contain a breach is between 216 and 327 days. While identifying a breach with delay causes the direct costs of the breach to accumulate until the breach is contained, it also generates indirect losses that are incurred by consumers and investors of the firm.

Moreover, firms have incentives to strategically underreport cyber incidents or delay announcing them (Amir et al, 2018). Delayed announcement of cyber breaches provides opportunistic trading windows. Garg (2020) find evidence that cyber breach informed-insiders engage in short-selling, while Piccotti and Wang (2022) find that hackers initiate informed trading up to 12 months prior to data breach announcements in the options markets. Similarly, Lin et al. (2020) show that the most opportunistic trading occurs 55-72 days before the breach announcements, and they estimate that insiders save an average of USD 35,000 due to short selling in the 3 months before the announcement.

3.5 Response Costs

Response costs are expenses incurred to address and mitigate the impact of the incident, encompassing a broad spectrum of direct, defense, and indirect costs that reflect the multifaceted impact of these incidents on firms. Cyber incidents can result in various types of response costs, from changes in leadership roles, to higher commitment to corporate social responsibility, and legal actions. For example, when faced with a cyber incident, organizations typically recruit an incident response team to investigate and contain the incident. The response teams help conduct forensic analysis to examine the affected systems and networks, identify the cause of the incident, and gather evidence for potential legal action. According to Burgard (2021), these costs range from USD 30,000 to USD 150,000. Similarly, organizations affected by cyber incidents may incur costs associated with legal and regulatory obligations. This type of response costs include hiring legal counsel, complying with data breach notification requirements, and potential fines or penalties for non-compliance. Burgard (2021) estimates that legal fees cost about USD 25,000, which may exponentially increase if the firm faces a lawsuit.

In this sense, the literature claims that victims do more than taking legal actions in response to a cyber breach, they adjust their behavior to counteract the damage to their reputation—a precautionary way to reduce financial loss over time. For instance, a study by Akey et al. (2021) reveals that attacked firms significantly increase their investment in corporate social responsibility, typically by 0.4-0.5 standard deviations, to mitigate the reputational losses incurred. Increased investment in corporate social responsibility and leadership changes highlight the gravity of cyber incidents and the extent firms may go to offset their effects. Garg (2020) demonstrates that in the U.S. both the affected firms and their suppliers, as well as the unaffected peer firms, tend to increase their cash holdings following a breach. This suggests a collective response to bolster financial stability in the face of cyber risks. Furthermore, Tosun (2021) discovers that firms that encounter a data breach tend to invest more in research and development (R&D), indicating a long-term commitment to improving their security measures. Additionally, these firms are also more inclined to make CEO changes. Mainly, attacked firms exhibit a higher likelihood of replacing their CEO and CTO, while also making efforts to enhance their social responsibility practices after experiencing a breach (Lending et al., 2018). Finally, there is also evidence showing that firms employ identity theft counter measures which is associated with a 0.63% increase in a firm's market value (Bose and Leung, 2013).

3.6 Costs arising from cyber risk

Cybersecurity risk is an important consideration for investment decisions. The presence of cyber risk may create indirect costs to the economy by affecting the allocation of resources and preventing the development of certain sectors. Business leaders rank cyber incidents as the top operational risk they face (World Economic Forum, 2022). Florackis et al. (2023) shows that cybersecurity risk is priced in equity prices.[10]

However, despite its importance in investment and firm value creation, the quantification of cyber risk proves even more challenging than data collection since it entails estimating both successful and failed attacks and formalizing a probability function (Woods and Moore, 2019). By reviewing the existing cyber risk indexes and tools (see Appendix 2), as well as the literature, we find that the literature on cyber risk is very limited, and that there is a lack of consistent data and methodologies to assess cyber risk. These limitations have driven researchers and stakeholders (e.g., insurance companies) to use new or more complex methods to quantify cyber risk. For example, Woods and Bohme (2021) systematizes the empirical research into cyber harm

[10] This means that firms with higher cybersecurity risk outperform others in regular times, but incur in large losses after the disclosure of a cyber breach.

estimates and the effectiveness of security interventions and use artificial data and a structural equation model to indirectly measure the realization of risk through losses.

Table 4 summarizes other findings and methods applied in key papers, including the determinants of risk. A striking study shows that firm-level cybersecurity risk can be a source of systematic risk in financial markets. This suggests that there are large externalities of a firm's cyber risk. The network effects may multiply an incident occurring in a single firm and may cause large disruptions in the entire financial system.

Lhuissier and Tripier (2021) show that the performance of cybersecurity companies increases during times with high cybercrime. However, the complex nature of cybersecurity risk makes it difficult for the private sector to adequately protect the cyberspace. The presence of externalities and network effects highlights the importance of recognizing cybersecurity as a public good.

Table 4: Summary of literature on measuring cybersecurity risk

Paper	Main findings with risk index of paper	Notes on methods	Sample	Period
Florackis et al. (2023)	Firms with higher risk outperform other firms by up to 8.3% per year in terms of equal-weighted (7.9% value-weighted) returns.	Textual analysis of annual corporate filings (10-K)	United States	2008-2019
Facchinetti et al. (2020)	The riskiest combinations of an attack are those associated with 0-day, Phone Hacking and Vulnerabilities, in combination with Espionage and Information Warfare.	Theoretical	N/A	N/A
Lhuissier and Tripier (2021)	The rise of cybercrime is positively correlated with the performance of cybersecurity companies.	Scraping all tweets world-wide that contain both "cyber" and "risk", "attack", or "threat"	Global (not broken by countries)	2011-2020
Jamilov et al. (2021)	Firm-level cybersecurity risk can be a source of systematic risk in financial markets.	Textual analysis of quarterly earnings announcement & Q&A sessions	85 countries	2002-2021
Bouveret (2018)	Cybersecurity threats are growing for financial institutions. Given the reliance of their operations on technology, Fintech firms are particularly vulnerable to cyber risks.	Their index consists of the number of Factiva articles featuring "cyberattack" or "hack" or "cyber risk" or "cyber security" and "banks" or "bank" and "risk" divided by the number of articles featuring "banks" or "bank" and "risk" by country.	Global (broken by countries)	2014-2017
Keppo and Niemelan(2021)	Hacking campaigns increase the target institutions' exposure to deep web and dark web by 62% per year during the first two years after the campaign's start date.	Over 200 million dark web and deep web pages	460 financial institutions in 167 countries that are targeted by 9 ideologically motivated campaigns	2012-2018

Source: Authors' own elaboration

4 Challenges of studying the costs of cyber incidents

This literature review identifies the lack of open reliable data on cyber incidents as the major challenge for doing research in this field (Anderson et al., 2013; Chen et al., 2023; Kigerl, 2016), mainly, in developing countries. Most of the data on major cyber incidents come either from the compliance of disclosure mandates or the work of intelligence offices (e.g., U.S.). Moreover, these data often have under-reporting or under-recording issues (Howell and Burrus, 2020), limiting the scope of analysis to developed countries like the U.S. (e.g., Amir et al., 2018; Akey et al., 2021; Kamiya et al., 2021; Lending et al., 2018; Piccotti and Wang, 2022; Lin et al., 2020; Tosun, 2021), where there is more and better-quality data. For example, the Privacy Rights Clearinghouse (PRC) provides open data on all cyber breaches made public by government entities in the U.S. since 2004, which have informed some of the most influential papers in the field (Amir et al., 2018; Akey et al., 2021; Kamiya et al., 2021; Lending et al., 2018; Piccotti and Wang, 2022; Lin et al., 2020; Tosun 2021).[11] In the context of developing countries, however, such datasets are significantly missing. A popular but confidential dataset available for the whole world is the consortium data provided by ORX, which only covers operational risks by financial institutions. New attempts to gather data on cyber incidents are using A.I. to scrape social media and news articles and identify disclosed cyber incidents around the world (Altalhi and Gutub, 2021; Harry and Gallagher (2018); Vergara et al., forthcoming).

There are at least five reasons why it is challenging to record, merge, and measure cyber incidents. First, we find non-standardized definitions of cybersecurity concepts (e.g., cyber incidents and systemic cybersecurity risk). For example, some define cyber incidents as traditional crimes that are facilitated by utilizing information communication technology (ICT) as well as new crimes that emerge with the arrival of computational-based technologies (Ho and Luong, 2022). Others define cyber incidents as a subclass of general operational risk events (Aldasoro et al., 2020), while others define them as industry events with the risk of affecting technological assets (Biener et al., 2015). Agreeing on an exact definition of cyber incidents would allow for a correct identification of important cybersecurity measures like systemic cybersecurity risk. To our understanding, perhaps, the most comprehensive definition of a cyber incident is that it is "any human attempt to disrupt the cyberspace with an economic, malicious, or harmful intention, where the cyberspace is the domain composed of "all digital networks used to store, modify, and communicate information" and which may or may not result in economic losses" (Biener et al., 2015).[12] This definition aligns with the European Commission's 2007 concept of cybercrime that encompasses traditional crimes via ICTs, and electronic-network-specific crimes like DDoS, hacking, and malware..

Second, regulation for the disclosure of cyberattacks and other cybersecurity regulations differ across regions and time. For example, the General Data Protection Regulation (GDPR) of the European Union requires firms to disclose breaches within 72 hours. While the U.S. Securities and Exchange Commission mandates public companies to report cyber incidents within 96 hours after detection of the event. Moreover, while 99% of European countries have data protection legislation, only 65% of African countries have implemented such measures. Similarly, while 85% of European nations have breach notification measures only 34% of countries in the Americas, 42% of countries in Asia Pacific, and 43% in Africa have adapted such legislations (ITU, 2021).[13]

---

[11] Advisen, Audit Analytics, and Gelmato are other popular but confidential data sources in the U.S.

[12] Cybersecurity breaches and attacks can be both understood as forms of incidents—though breach es can occur for other reasons beyond cyber-attacks, which in turn do not necessarily result in breaches. Either way, cybercrime and cybersecurity breaches overlap significantly in terms of associated costs (Heyburn, Shah, & Furnell, 2020).

[13] For more information on the 2020 ITU Global Cyber Security Index, see: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Third, cyber incidents targeting citizens are not systematically reported and are even harder to track down. Attacks on individuals may have important physical and non-physical costs like the damages to computers and phones, as well as loss of important documents and personal data, attention, and productivity.

Fourth, it usually takes time until an entity notices their exposure to a cyberattack, which renders challenging the process of identifying the exact date of the event. According to IBM (2022), the average time to identify and contain a data breach ranges between 216 and 327 days. This implies that even when there are cyber breaches disclosure rules, uncertainty remains about the exact time when the breach happened.

Finally, as documented by Amir et al. (2018), there is strategic underreporting by firms in disclosing cyber breaches.[14] Facchinetti et al. (2020) suggests that one way to prevent underreporting by firms is to require them to report ordinal information on the severity of the attack rather than focusing on the quantification of the losses of the attack, because reporting only the severity of the attack reduces the legal and recovery costs of a firm following the disclosure of a breach. Therefore, firms would have greater incentives to report when they do not have to inform the authorities of the exact amounts of the losses.

5 Conclusions and Discussion on Policy Recommendations

This paper analyzes the economic costs of cyber incidents recorded in 15 prominent global-spanning cybersecurity reports from industry and government stakeholders and over 50 academic papers by leading scholars tackling issues on the economics of cybersecurity. We identify that the economic costs of a threat to the cyberspace extend well beyond the immediate costs of cybercrime, creating also indirect costs that could be as important as the former, as well as continuous response costs.

The non-scholarly literature has presented a vast range of aggregate estimations of the total costs of cyber incidents ranging from USD 172 billion in 2017 to USD 8.0 trillion in 2021, and even climbing to as high as USD 10.5 trillion by 2025 (about 9.1% of the global GDP). However, our review shows that the validity of these cost estimates cannot be verified as many of these sources do not back their finding with well-explained methodologies. This could lead to mis-informed decision making since these estimates play an important role as a baseline for cost-benefit analyses (CISA, 2021). Moreover, our analytical survey reveals that the economic losses of cyber incidents go beyond the immediate quantifiable costs since cyber incidents often incur in indirect costs that have often remain unmeasured. For example, our survey reveals that cyber incidents can translate into systemic risk in financial markets, contagion effects to other firms in the same industry, and volatility in both domestic and global stock markets. However, given the lack of global open, accurate, and reliable data on disclosed and non-disclosed cyber incidents, the community has yet to find a credible estimate for the real global costs of cyber incidents.

Besides the problem of credible estimates, this literature also identifies an important gap in cybersecurity knowledge for developing countries, with over 90% of the reviewed literature focusing on developed countries, mainly, the U.S. This imbalance potentially skews the analytical outcomes regarding the true economic costs of cyber incidents and associated policy implications. To address this issue, further data, tools, and improved analytical approaches are needed to better understand the impact of cyber incidents on economies across the world.

[14] Amir et al. (2018) compares the characteristics of firms which voluntarily disclose to firms who choose to withhold information on cyberattacks. They find that managers disclose information on cyberattacks when investors already suspect a high likelihood of an attack. Withholding firms have less analyst coverage, weaker corporate governance, and lower litigation risk than disclosing firms.

In terms of policy implications, this literature review identifies two major issues. First, the lack of reliable data on cyber incidents is the major factor that prevents researchers from obtaining precise estimates of the economic effects of cyber incidents. The existing databases (e.g., the U.S. PRC database) report disclosed incidents only for specific industries in developed countries, mainly the U.S. Academic studies that use these datasets provide credible estimates of particular aspects of cybersecurity incidents such as the stock market effects. Nevertheless, these studies remain insufficient for understanding the economy-wide impacts of cyber incidents. There is particularly little understanding of the effects of cyber incidents in developing countries, as the available data sources do not cover them. Therefore, there is a need for international cooperation to standardize the systems for reporting and classifying cyber incidents globally.

Second, acknowledging some aspects of cybersecurity as a public good is critical due to the systemic risk that cyber incidents can pose to financial systems, supply chains, critical infrastructure, amongst others. Moreover, the market failures intrinsic to cybersecurity such as the externalities posed by the targeted firm to their clients and suppliers underscore the need for recognizing cybersecurity as a public good. Governments across the world are in a prime position to foster stronger cybersecurity outcomes. By encouraging the creation of secure technologies and investing in public and national security, they can enhance the protection of vital infrastructure for societal and economic resilience.

In conclusion, the key findings from the proposed literature survey emphasize the necessity for a comprehensive, empirical, and multidisciplinary approach rooted in data to understand, measure, and mitigate the economic costs associated with cyber incidents. At the firm and country levels, the question remains, "How do we know this is a good investment among the myriad of options we could potentially invest in? How can we improve at developing effective metrics to help boards make better-informed decisions?" (WEF, 2023). By adopting evidence-based metrics and a risk-based approach, stakeholders could further understand the returns to cybersecurity investments.

References

[1] Hamid, N.H.A.A., Ibrahim, N., Nor, M., Hussain, F.M., Raju, R., Naseer, H. and Ahmad, A., 2022. Barriers and enablers to adoption of cyber insurance in developing countries: An exploratory study of Malaysian organizations. *Computers & Security*, 122, p.102893.

[2] Aboal, D. and Tacsir, E., 2015. Innovation and productivity in services and manufacturing: The role of ICT investment (No. IDB-WP-658). *IDB Working Paper Series*.

[3] Accenture & Ponemon Institute (2019). Securing the Digital Economy Report. Available at: https://www.accenture.com/us-en/insights/cybersecurity/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf#zoom=50

[4] Acquisti, A., Friedman, A. and Telang, R. (2006) 'Is there a cost to privacy breaches? An event study', *ICIS 2006 proceedings*, pp. 94.

[5] Africa Center for Strategic Studies (2021). Africa's Evolving Cyber Threats. Available at: https://africacenter.org/spotlight/Africa-evolving-cyber-threats/

[6] Aker, J.C. and Mbiti, I.M., 2010. Mobile phones and economic development in Africa. *Journal of Economic Perspectives*, 24(3), pp.207-32.

[7] Akey, P., Lewellen, S., Liskovich, I., & Schiller, C. (2021) 'Hacking corporate reputations', *Rotman School of Management Working Paper*, (3143740).

[8] Aldasoro, I., Gambacorta, L., Giudici, P. and Leach, T. (2020) 'Operational and cyber risks in the financial sector'. *BIS Working Papers*. No. 840.

[9] Aldasoro, I., Gambacorta, L., Giudici, P. and Leach, T. (2022) 'The drivers of cyber risk', *Journal of Financial Stability*, 60, 100989.

[10] Allen, F., Gu, X. and Jagtiani, J. (2021) 'A survey of fintech research and policy discussion', *Review of Corporate Finance*, 1, pp. 259-339.

[11] Altalhi, S. and Gutub, A., 2021. A survey on predictions of cyber-attacks utilizing real-time twitter tracing recognition. *Journal of Ambient Intelligence and Humanized Computing*, pp.1-13.

[12] Amir, E., Levi, S., & Livne, T. (2018) 'Do firms underreport information on cyber-attacks? Evidence from capital markets', *Review of Accounting Studies*, 23, pp. 1177-1206.

[13] Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M.J., Levi, M., Moore, T. and Savage, S., 2013. Measuring the cost of cybercrime. *The economics of information security and privacy*, pp.265-300. Springer.

[14] Austin, G. and Withers, G. (2021) 'Valuation of Reputation Damage for Transport Cyber Attack'. Working Paper.

[15] Australian Strategy Policy Institute (2017). Cyber Maturity in the Asia-Pacific Region. Available at: ttps://s3-ap-southeast-2.amazonaws.com/ad-aspi/2017-12/ASPI Cyber Maturity 2017_AccPDF_FA_opt.pdf?hDv5_AxfVWgwCA_q8it1_H1wkH_HwZjb

[16] Belfer Center for Science and International Affairs, Harvard Kennedy School of Government (2022). Available at https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf

[17] Biener, C., Eling, M. and Wirfs, J. H. (2015) 'Insurability of cyber risk: An empirical analysis', *The Geneva Papers on Risk and Insurance-Issues and Practice*, 40, pp. 131-158.

[18] Bose, I., & Leung, A. C. M. (2013) 'The impact of adoption of identity theft countermeasures on firm value', *Decision Support Systems*, 55(3), pp. 753-763.

[19] Bouveret, A. (2018) 'Cyber risk for the financial sector: A framework for quantitative assessment', *International Monetary Fund.*

[20] *Burgard, M. (2021) "Cyber Incident Response: The Real Cost of Not Having a Plan or Cyber Insurance."* Available at: https://www.marconet.com/blog/cyber-incident-response#:~:text=Incident%20response%20firms,come%20out%20of%20your%20pocket.

[21] Campbell, K., Gordon, L. A., Loeb, M. P. and Zhou, L. (2003) 'The economic cost of publicly announced information security breaches: empirical evidence from the stock market', *Journal of Computer Security,* 11(3), pp. 431-448.

[22] Cavusoglu, H., Mishra, B. and 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), pp. 70-104.

[23] CGTN (2020). Unveiling the cost of cybercrime in Africa. Available at: https://news.cgtn.com/news/2020-10-27/Unveiling-the-cost-of-cybercrime-in-Africa-UVhmu1PJeM/index.html

[24] CheckPoint—Software Technologies LTD (2021). Cybersecurity Report. Available at: https://technologyconcepts.com/wp-content/uploads/2021/10/cyber-security-report-2021.pdf

[25] Corbet, S. and Gurdgiev, C. (2019) 'What the hack: Systematic risk contagion from cyber events', *International Review of Financial Analysis*, 65, 101386.

[26] Crosignani, M., Macchiavelli, M., & Silva, A. F. (2023) 'Pirates without borders: The propagation of cyberattacks through firms' supply chains', *Journal of Financial Economics*, 147(2), pp. 432-448.

[27] Coyne, C.J. and Leeson, P.T., 2017. Who's to protect cyberspace?. In *Computer Crime* (pp. 507-530). Routledge.

[28] Cybereason (2022). Ransomware: The Ture Cost to Businesses. Available at: https://www.cybereason.com/hubfs/dam/collateral/reports/Ransomware-The-True-Cost-to-Business-2022.pdf

[29] CyberGreen (n.d.) Cyber Green Index. Available at: https://stats.cybergreen.net/

[30] Dou, W., Tang, W., Wu, X., Qi, L., Xu, X., Zhang, X. and Hu, C., 2020. An insurance theory based optimal cyber-insurance contract against moral hazard. *Information Sciences*, 527, pp.576-589.

[31] eSentire & Cybersecurity Ventures (2019). Official Annual Cybercrime Report. Available at: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

[32] eSentire & Cybersecurity Ventures (2022). Official Cybercrime Report. Available at: https://s3.ca-central-1.amazonaws.com/esentire-dot-com-assets/assets/resourcefiles/2022-Official-Cybercrime-Report.pdf

[33] European Parliament (2021). Cybersecurity: understanding the threats and addressing the challenges. Available at: https://www.europarl.europa.eu/pdfs/news/expert/2021/10/story/20211008STO14521/20211008STO14521_en.pdf

[34] Facchinetti, S., Giudici, P. and Osmetti, S.A., 2020. Cyber risk measurement with ordinal data. *Statistical Methods & Applications*, 29, pp.173-185.

[35] Florackis, C., Louca, C., Michaely, R. and Weber, M. (2023) 'Cybersecurity risk', *The Review of Financial Studies*, 36(1), pp. 351-407.

[36] Garg, A., Curtis, J., & Halper, H. (2003) 'Quantifying the financial impact of IT security breaches', *Information Management & Computer Security*, 11(2), pp. 74-83.

[37] Garg, P. (2020) 'Cybersecurity breaches and cash holdings: Spillover effect', *Financial Management*, 49(2), pp. 503-519.

[38] Global Cyber Security Capacity Centre, University of Oxford (2021). Cybersecurity Capacity Maturity Model for Nations (CMM). Available at: https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

[39] Goldstein, J., Chernobai, A., & Benaroch, M. (2011) 'An event study analysis of the economic impact of IT operational risk and its subcategories', *Journal of the Association for Information Systems*, 12(9), pp. 1-23.

[40] Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L., 2015. Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, 1(1), pp.3-17.

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

[42] Gordon, L.A., Loeb, M.P. and Zhou, L., 2020. Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity*, *6*(1), p.ty005.

[43] Grant Thorton (2021). The Economic Cost of Cybercrime. Available at: https://www.grantthornton.ie/globalassets/1.-member-firms/ireland/insights/publications/grant-thornton---the-economic-cost-of-cybercrime.pdf

[44] Harry, C., & Gallagher, N. (2018). Classifying cyber events. *Journal of Information Warfare*, 17(3), 17-31

[45] Heyburn, H., Shah, J. N., & Furnell, S. (2020). Analysis of the full costs of cyber security breaches: Final Report. *Ipsos MORI*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/901569/Analysis_of_the_full_cost_of_cyber_security_breaches.pdf

[46] Hiscox (2022). Cyber Readiness Report. Available at: https://www.hiscoxgroup.com/sites/group/files/documents/2022-05/22054 - Hiscox Cyber Readiness Report 2022-EN_0.pdf

[47] Ho, H.T.N. and Luong, H.T., 2022. Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis. *SN Social Sciences*, 2(1), p.4.

[48] 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), pp. 97-121.

[49] Howell, C.J. and Burruss, G.W., 2020. Datasets for analysis of cybercrime. *The Palgrave handbook of international cybercrime and cyberdeviance*, pp.207-219.

[50] IBM (2022). Cost of a Data Breach Report. Available at: https://www.ibm.com/reports/data-breach

[51] IC3 (2017). Internet Crime Report. Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2017_IC3Report.pdf

[52] IC3 (2019). Internet Crime Report. Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf

[53] IC3 (2020). Internet Crime Report. Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[54] International Telecommunication Union (ITU) (2021). Global Cybersecurity Index (GCI). Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

[55] Interpol (2021). African Cyberthreat Assessment Report. Available at: https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf

[56] Iyer, S. R., Simkins, B. J., & Wang, H. (2020) 'Cyberattacks and impact on bond valuation', *Finance Research Letters,* 33, 101215.

[57] Jamilov, R., Rey, H. and Tahoun, A. (2021) 'The anatomy of cyber risk' (No. w28906), *National Bureau of Economic Research*.

[58] Kamiya, S., Kang, J. K., 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), pp. 719-749.

[59] Kannan, K., Rees, J., & Sridhar, S. (2007) 'Market reactions to information security breach announcements: An empirical analysis', *International Journal of Electronic Commerce*, 12(1), pp. 69-91.

[60] Kapersky Lab & B2B (2017). Damage Control: The Cost of Security Breaches. Available at: https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf

[61] Kapersky Lab (2021). IT Security Economics Report. Available at: https://go.kaspersky.com/rs/802-IJN-240/images/Kaspersky_IT%20Security%20Economics_report_2021.pdf

[62] Kashyap, A. K., & Wetherilt, A. (2019). Some principles for regulating cyber risk. *AEA Papers and Proceedings*, 109, 482-487.

[63] Keppo, Jussi and Niemela, Mikko, Do Hacker Groups Pose a Risk to Organizations? Study on Financial Institutions Targeted by Hacktivists (July 1, 2021). Available at *SSRN*: https://ssrn.com/abstract=3835547

[64] Kigerl, A., 2016. Cyber Crime Nation Typologies: K-Means Clustering of Countries Based on Cyber Crime Rates. *International Journal of Cyber Criminology*, *10*(2).

[65] Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber risk, market failures, and financial stability. *International Monetary Fund.*

[66] Kotidis, Antonis, and Stacey L. Schreft (2022). "Cyberattacks and Financial Stability: Evidence from a Natural Experiment," Finance and Economics Discussion Series 2022-025. Washington: *Board of Governors of the Federal Reserve System*, https://doi.org/10.17016/FEDS.2022.025.

[67] Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77-81.

[68] Lending, C., Minnick, K., & Schorno, P. J. (2018) 'Corporate governance, social responsibility, and data breaches', *Financial Review*, 53(2), pp. 413-455.

[69] Lhuissier S. and Tripier, F. (2021) 'Measuring Cyber Risk'. Working Paper.

[70] Lin, Z., Sapp, T. R., Ulmer, J. R., & Parsa, R. (2020). Insider trading ahead of cyber breach announcements. *Journal of Financial Markets*, 50, 100527.

[71] Makridis, C. A. (2021) 'Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018', *Journal of Cybersecurity*, 7(1), tyab021.

[72] McAfee & Center for Strategic and International Studies (2018). Economic Impact of Cybercrime Report. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

[73] Ministry of Foreign Affairs, Estonia (2018). *National Cyber Security Index (NCSI).* Available at: https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf

[74] MIT Technology Review (2022). Cyber Defense Index (CDI). Available at: https://mittrinsights.s3.amazonaws.com/CDIreport.pdf

[75] Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5), 1938-1940.

[76] NetDiligence (2022). Cyber Claims Study. Available at: https://netdiligence.com/wp-content/uploads/2022/10/NetD_2022_Claims_Study_1.0_PUBLIC.pdf

[77] Norton (2017). Cyber Security Insights Report Global Results. Available at: https://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/CSIR-global-results-US.pdf

[78] Phys.org (2021). Rights group has new tool to stem cybercrime in Africa. Available at: https://phys.org/news/2021-05-rights-group-tool-stem-cybercrime.html

[79] Piccotti, L. R., & Wang, H. (2022) 'Informed trading in the options market surrounding data breaches', *Global Finance Journal*, 100774.

[80] Plonka, M., Niżnik, J. and Jedynak, T., 2023. Health security as a public good in the era of the Fourth Industrial Revolution in Poland. In *Public Goods and the Fourth Industrial Revolution*. Taylor & Francis.

[81] Privacy Rights Clearinghouse. (2002) Privacy Rights Clearinghouse PRC. United States. [Web Archive] Retrieved from the Library of Congress, https://www.loc.gov/item/lcwaN0009136/.

[82] PwC (2018). The growing market for cyber insurance. Available at: https://www.pwc.com/us/en/industry/assets/pwc-cyber-insurance-survey.pdf

[83] Romanosky, S., Ablon, L., Kuehn, A. and Jones, T., (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk?. *Journal of Cybersecurity*, *5*(1), p.tyz002.

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

[85] Saputra, P. N., Sudirman, A., Sinaga, O., Wardhana, W., & Hayana, N. (2019). Addressing Indonesia's Cyber Security through Public-Private Partnership (PPP). *Central European Journal of International & Security Studies*, *13*(4).

[86] Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, 58, 216-229.

[87] Symantec (2019). Internet Security Threat Report. Available at: https://docs.broadcom.com/doc/istr-24-2019-en

[88] Taddeo, M., 2019. Is cybersecurity a public good?. *Minds and Machines*, 29, pp.349-354.

[89] Tenable Network Security (2017). Global Cybersecurity Assurance Report Card. Available at: Available at: https://cyber-edge.com/resources/tenable-2017-global-cybersecurity-assurance-report-card/

[90] Thompson, E.C., 2018. Cybersecurity incident response: How to contain, eradicate, and recover from incidents. *Apress*.

[91] Tosun, O. K. (2021) 'Cyber-attacks and stock market activity', *International Review of Financial Analysis,* 76, 101795.

[92] UK Cabinet Office (2011). The Cost of Cyber Crime: A Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf

[93] U.S. CISA (U.S. Cybersecurity and Infrastructure Security Agency) (2021). Cost of Cyber Incidents Study. Available at: https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf

[94] Verizon (2022). Data Breach Investigations Report. Available at: https://www.verizon.com/business/resources/Tcfa/reports/dbir/2022-data-breach-investigations-report-dbir.pdf

[95] Wang, H. E., Wang, Q. E., & Wu, W. (2022) 'Short selling surrounding data breach announcements', *Finance Research Letters*, 47, 102690.
[96] Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research*, 24(2), 201-218.
[97] Willis Towers Watson (2020). Cyber Claims Analysis Report. Available at: https://www.wtwco.com/en-NZ/Insights/2020/07/cyber-claims-analysis-report
[98] Woods, D.W. and Böhme, R., 2021, May. SoK: Quantifying cyber risk. In *2021 IEEE Symposium on Security and Privacy (SP)* (pp. 211-228). IEEE.
[99] Woods, D.W. and Moore, T. (2019). Does insurance have a future in governing cybersecurity?. *IEEE Security & Privacy*, 18(1), pp.21-27.
[100] Woods, D. W., Moore, T. and Simpson, A. C. (2021) 'The county fair cyber loss distribution: Drawing inferences from insurance prices', *Digital Threats: Research and Practice*, 2(2), pp. 1-21.
[101] World Economic Forum (2022). Cyber Resilience Index (CRI): Advancing Organizational Cyber Resilience. Available at: https://www.weforum.org/whitepapers/the-cyber-resilience-index-advancing-organizational-cyber-resilience/
[102] World Economic Forum (2023). Global Security Outlook 2023. Available at: https://www.weforum.org/reports/global-cybersecurity-outlook-2023

Appendix I: Main estimations on the economic costs of cybersecurity incidents from industry stakeholders, 2017-2023

Table A2: Summaries of reviewed industry reports

The Cost of a Data Breach *IBM* **(2022)**	
Summary	The IBM report on data breaches examines the impact and cost of data breaches on organizations using data from real-world incidents—excluding very small and very large data breaches to avoid the results to be skewed. Data breaches examined in the 2022 version ranged in size between 2,200 and 102,000 compromised records. In-depth qualitative also comprised of over 3,600 separate interviews with staff at 550 organizations between 2021 and 2022. The report identifies key factors that influence the cost of data breaches, including the size of the breach, the time it takes to identify and contain the breach, and the use of certain security measures. The study also highlights the importance of incident response planning and the need for organizations to prioritize their security investments. In conclusion, the report emphasizes the critical need for organizations to invest in proactive security measures and comprehensive incident response plans to mitigate the impact and cost of data breaches.
Key highlights on the economic impacts of cybersecurity incidents	❖ In 2022, the average data breach cost reached an all-time high of USD 4.35 million, marking a 2.6% increase from the previous year's USD 4.24 million. This represents a 12.7% rise since the 2020 report, when the average cost was USD 3.86 million. ❖ Six of the 17 countries/regions analyzed (Germany, Japan, France, South Korea, Scandinavia, and Türkiye) experienced a decline in average data breach costs in comparison to the 2021 findings, with Brazil having the largest relative cost increase (27.8%, from USD 1.08 million to USD 1.38 million) and Türkiye experiencing the biggest cost decrease (42%, from USD 1.91 million to USD 1.11 million). ❖ The 5 countries/regions with the highest average data breach costs in the 2022 findings include the United States (USD 9.44 million), the Middle East (USD 7.46 million), Canada (USD 5.64 million), the United Kingdom (USD 5.05 million), and Germany (USD 4.85 million). The U.S. topped the list for 12 consecutive years. ❖ Based on the data of the 550 organizations analyzed worldwide, ransomware breach costs have slightly decreased from USD 4.62 million in 2021 to USD 4.54 million in 2022. However, the occurrence of ransomware breaches has increased by 11% in the 2022 study compared to the 2021 findings. The average cost of a destructive or wiper attack

	was USD 5.12 million in 2022, which was USD 0.77 million more than the global average total cost of a data breach of USD 4.35 million in the same period. ❖ In the 2022 findings drawn from the 550 worldwide firms, fully deployed security AI and automation were associated with significantly lower average breach costs (USD 3.15 million) compared to organizations without these measures (USD 6.20 million); mature organizations experienced lower average breach costs (USD 3.87 million) than those in the early stages of securing their cloud environments (USD 4.53 million). ❖ Healthcare breach costs reached a record high, with an average cost of USD 10.10 million, an increase of nearly USD 1 million from the 2021 estimates. Moreover, healthcare has been the costliest industry for breaches for 12 consecutive years, with a 41.6% increase since 2020. ❖ Financial organizations ranked second, averaging USD 5.97 million, followed by pharmaceuticals (USD 5.01 million), technology (USD 4.97 million), and energy (USD 4.72 million). ❖ Critical infrastructure organizations had an average data breach cost of USD 4.82 million in the 2022 study, which was USD 1 million higher than organizations in other industries. These organizations encompass financial services, industrial, technology, energy, transportation, communication, healthcare, education, and public sector industries. ❖ In the 2022 study, mature organizations experienced lower average breach costs of USD 0.66 million compared to those in the early stages of securing their cloud environments. Mature-stage organizations had an average cost of USD 3.87 million, while mid-stage organizations faced USD 4.39 million, early-stage organizations saw USD 4.53 million, and those yet to start their cloud security journey incurred USD 4.59 million. The cost difference between mature and early-stage organizations represented a 15.7% savings for mature-stage organizations.
Economic Impact of Cybercrime Report *McAfee & Center for Strategic and International Studies (CSIS)* (2018)	
Summary	The report examines the significant impact of cybercrime on global economies. It reveals that the global cost of cybercrime has increased, totaling USD 600 billion in 2018. It provides an overview of the types of cybercrime, such as theft of intellectual property, personal information, and financial data, and outlines the ways in which businesses, governments, and individuals can protect themselves. The report concludes that cybercrime is a significant global threat that requires urgent attention and action.
Key highlights on the economic impacts of cybersecurity incidents	❖ Estimates for the cost of cybercrime vary significantly, ranging from tens of billions to over a trillion dollars, due to limited data and differing methodologies. This modeling effort estimates that the global cost of cybercrime may be as much as USD 600 billion (with the range being between USD 445 billion and USD 600 billion). According to the 2018 estimates in which the study was based on, this means that nearly to up one percent of global GDP is lost to cybercrime each year, which is up from a 2014 study that put global losses at about USD 445 billion. ❖ The United Arab Emirates (UAE) Cyber Security Centre ranks the country as the second most targeted country for cyberattacks. High internet penetration, technological sophistication, and visibility contribute to UAE's annual cybercrime cost of USD 1.4 billion, according to 2018 estimates. ❖ CSIS identifies five trends that have significantly contributed to the increase in cybercrime in the last three years. These include state-sponsored bank robbery, the rise of ransomware, the emergence of Cybercrime-as-a-Service, increased use of anonymization services like Tor and digital currencies, and the widespread theft of personal information and intellectual property (IP). ❖ Global Financial Integrity estimated that in 2017, transnational crime cost the world between USD 1.6 trillion and USD 2.2 trillion. Cybercrime accounted for approximately one-seventh of these costs—meaning a monetary estimate ranging from 228.6 billion and 314.3 billion USD. ❖ According to German IT industry association Bitkom, more than half of all German companies have been the victims of cybercrime, causing damages of more than USD 64 billion per year in 2018.
Securing the Digital Economy Report *Accenture/Ponemon Institute* (2019)	
Summary	This annual report offers a comprehensive analysis of the current state of cybersecurity in the digital economy. The report identifies the increasing frequency and sophistication of cyberattacks as a major threat to global economic growth and the digital ecosystem. Accenture advocates for a reinvention of the internet to prioritize trust and security, with a focus on three key areas: cybersecurity, privacy, and digital identity. The main conclusion of the report is that businesses and governments must take proactive steps to secure the digital economy and protect the privacy and trust of users.

Key highlights on the economic impacts of cybersecurity incidents	❖ In the private sector, over the next five years, companies face the risk of losing an estimated USD 5.2 trillion in value creation opportunities from the digital economy due to cybersecurity attacks. This amount is nearly equivalent to the combined economies of France, Italy, and Spain. ❖ This equates to a 2.8% loss in revenue growth over the next five years for a large global company. High-tech industries face the greatest risk, with over USD 753 billion at stake.
Cyber Readiness Report *Hiscox* (2022)	
Summary	The report examines the cyber risks and challenges businesses face in today's world, with over 20 years of experience in privacy and cyber insurance to back up its findings. One of its main findings is that businesses are becoming more vulnerable to cyberattacks as more employees work from home, with 62% of respondents agreeing that their business is at greater risk and that number increasing to 69% for firms with over 250 employees. The report also found that 63% of UK businesses that were victims of a ransomware attack ended up paying the ransom. Overall, the report highlights the need for businesses to increase their cybersecurity measures and adopt a proactive approach to addressing these risks.
Key highlights on the economic impacts of cybersecurity incidents	❖ One-in-five firms paid substantial fines to a government agency because of a breach, doubling when compared to the 2021 estimates. ❖ Based on the survey data from 1,500 firms from U.S., France, Germany, Belgium, Spain, The Netherlands, and Ireland, the median cost of an attack has risen 29% to just under USD 17,000 in comparison to the 2021 estimates. ❖ In the analyzed countries, companies that purchased or enhanced cybersecurity insurance after an attack over the past 12 months tripled. Moreover, companies with 10 to 49 employees have reduced their cybersecurity budgets by almost 50%, from USD 411,000 to USD 225,000. For those with less than 10 employees, spending has declined significantly, from an average of USD 150,000 to just USD 29,000. This decrease is most likely due to the pandemic, as companies have less funds available to spend on IT. ❖ Compared to the previous year, a higher percentage of firms (19% vs. 16%) experienced ransomware attacks, with the U.S. and Irish firms being the most likely to pay the ransom, while German firms were the least likely. Two-thirds of affected firms paid the ransom, and over half paid on multiple occasions. Although only 14% of firms in the food and drink sector reported being targeted, it was found that 62% of affected firms in that sector gave in to paying the ransom, which was an interesting anomaly. The largest ransom paid was just under USD 100,000, a small increase from the previous year's USD 95,000.
Data Breach Investigations Report *Verizon* (2022)	
Summary	The report analyzes 23,896 incidents and confirms 5,212 data breaches that occurred between November 2020 and October 2021. The report highlights that healthcare has become a prime target for hackers. Ransomware attacks are on the rise, with the discovery method of Actor Disclosure becoming increasingly common. The report emphasizes the importance of businesses understanding the cybersecurity threats they face to minimize the risk of breaches and protect their assets and reputation.
Key highlights on the economic impacts of cybersecurity incidents	❖ In 2021, the U.S. Secret Service tackled transnational cybercrime activities, participating in multinational operations and allegedly preventing over USD 2.3 billion in economic losses from cyber incidents in the previous fiscal year.
Cyber Claims Study *NetDiligence* (2022)	
Summary	The NetDiligence 2022 Cyber Claims Study is a report analyzing over 7,000 cybersecurity claims from the period of 2017-2021. The report identifies the top cybersecurity threats affecting businesses and industries, such as phishing, ransomware, and business email compromise. It also highlights the industries with the highest claims frequency, including healthcare, education,

	and finance. The main conclusion of the report is that cybersecurity threats continue to pose a significant risk to businesses, and the cost of responding to these incidents is on the rise.
Key highlights on the economic impacts of cybersecurity incidents	❖ The study reveals that the average cost of a ransomware incident, including Business Interruption (BI) and recovery costs, is USD 623,000 for small and medium enterprises (SMEs) and USD 29.6 million for large companies. Furthermore, the five-year average cost of a claim involving BI was nearly four times higher than a claim without these additional expenses. ❖ In the analyzed period (2017-2021), ransomware incidents made up 87% of claims with a business interruption (BI) component for SMEs. Over five years, the average BI cost for ransomware incidents was USD 321,000, with a total incident cost of USD 623,000. In 2021, these figures rose to USD 756,000 for BI costs and USD 1.4 million for total incident costs, respectively. ❖ There was no consistent correlation between an organization's size and the extent of cybersecurity-related losses. Large companies experienced incidents up to 90 times costlier than those at SMEs. However, SMEs also faced significant losses, potentially with greater organizational impact, as 149 SME claims had total incident costs exceeding USD 1 million. No clear connection was observed between the number of records exposed and the total cost of an incident, except in the largest cases. Ransomware and business email compromise were the primary causes of loss, accounting for 44% of claims from 2017 to 2021 and nearly 50% in 2020 and 2021.
Official Cybercrime Report *eSentire & Cybersecurity Ventures* (2022)	
Main contributions	The report reveals that cybercrime has become more sophisticated and organized, leading to an increase in frequency and cost. The report identifies the top cybersecurity threats, including phishing, ransomware, and business email compromise, and the industries most targeted by these attacks, such as healthcare, finance, and manufacturing. The report also highlights the importance of proactive cybersecurity measures, including vulnerability management and employee training, to mitigate the risk of cybersecurity threats. The main contribution of the report is its comprehensive analysis of the current state of cybercrime and its impact on businesses, emphasizing the need for organizations to prioritize cybersecurity as a critical component of their overall risk management strategy.
Key highlights on the economic impacts of cybersecurity incidents	❖ Predicted to reach USD 8 trillion in 2023, the annual global cost of cybercrime surpasses natural disaster damages, outstrips the combined value of major illegal drug trades, and poses unparalleled threats to economic wealth transfer, innovation, and investment. ❖ Cybersecurity Ventures predicts global cybercrime damage costs will grow by 15 percent per year over the next five years, reaching USD 10.5 trillion annually by 2025, up from USD 3 trillion in 2015. ❖ According to the report, the cost of crypto crime worldwide is estimated to reach USD 30 billion per year by 2025. ❖ Ransomware attacks are expected to cause damages of approximately USD 265 billion per year by 2031, with a new attack every two seconds. The dollar figure is based on 30 percent year-over-year growth in damage costs over the next 10 years. ❖ A 2017 version of the report projected that ransomware damages would surge to USD 5 billion in 2017 from USD 325 million in 2015, a 15-fold jump in two years. The forecasted figures were USD 8 billion in 2018, USD 11.5 billion in 2019, and USD 20 billion in 2021, which was 57x higher than 2015.
IT Security Economics Report *Kaspersky Lab* (2021)	
Summary	The report highlights the significant financial impact of cyberattacks on businesses worldwide. The report shows that enterprises spent an average of USD 11.4 million on their IT security budget, while SMBs spent an average of USD 267,000. The main contribution of the report is to demonstrate the importance of investing in IT security and to provide businesses with insights into the financial consequences of cyberattacks. The conclusion is that businesses must prioritize their IT security budget to mitigate the risk of costly cyberattacks.

Key highlights on the economic impacts of cybersecurity incidents	❖ The cost of data breaches for SMEs increased slightly (USD 105,000 in 2021, compared to USD 101,000 in 2020, but still does not achieve the 2018 high point (USD 120,000). The cost of a data breach for enterprises fell to USD 927,000, below the previous low of USD 992,000 in 2017. ❖ Amid the pandemic, enterprise cybersecurity budgets planned at the end of 2020 dropped significantly by 19%, falling from USD 14 million in 2020 to USD 11.4 million in 2021. In contrast, SMEs security budgets experienced a minor decrease of 3%, with USD 267,000 in 2021 compared to USD 275,000 the previous year. ❖ Among all cybersecurity incidents, those affecting suppliers were the most expensive for SMEs, costing them USD 212,000 in 2021 alone. It was followed by attacks on point-of-sale (POS) systems; Supply chain attacks; electronic leakage of data from internal systems; Attacks on local / branch offices company (USD 209,000); crypto-mining attacks; and Incidents involving noncompeting, connected devices.
Internet Security Threat Report *Symantec* (2019)	
Main contributions	The report analyzes data from Symantec's Global Intelligence Network and provides insights into global threat activity, cybercriminal trends, and attacker motivations. Key findings from the report include the rise of form jacking attacks, the increasing use of living-off-the-land (LotL) techniques, and the growth of targeted ransomware attacks. The report also highlights the continued use of email as the primary infection vector for malware. Overall, the report provides a comprehensive analysis of the current threat landscape and offers valuable insights to help improve cybersecurity.
Key highlights on the economic impacts of cybersecurity incidents	❖ Ransomware infections overall decreased by more than 20% in the 2018-2019 period, but enterprise detections rose by 12%, indicating that ransomware remains an issue for enterprises. ❖ Symantec data revealed that according to its Global Intelligence Network, which collects data from millions of users worldwide, 4,818 unique websites were compromised with form jacking code every month in 2018. ❖ A single credit card's data can sell for up to USD 45 on underground markets; thus, cybercriminals could potentially generate up to USD 2.2 million monthly by stealing just 10 credit cards from compromised websites.
Damage Control: The Cost of Security Breaches *Kapersky Lab and B2B* The cost of security breaches (2017)	
Summary	This report by Kaspersky is based on a survey of 5,500 companies in 26 countries around the world and analyzes the financial impact of security breaches. The report reveals that enterprises, on average, spend more than half a million USD to recover from a security breach, while SMEs face an average loss of USD 38,000. These costs are only direct losses, and indirect damages, such as additional staff hiring and infrastructure upgrades, average USD 69,000 for large businesses and USD 8,000 for SMES. The report also identifies incidents involving third-party contractors, employee fraud, cybersecurity espionage, and network intrusion as the most damaging for large companies, with average losses significantly higher than other security incidents. The report concludes that investing in security measures is more cost-effective than recovering from security breaches.
Key highlights on the economic impacts of cybersecurity incidents	❖ In 2017, enterprises incur an average direct cost of USD 551,000 to recover from a security breach, while small and medium-sized businesses (SMBs) face an average cost of USD 38,000. ❖ Indirect costs resulting from a cybersecurity breach, including additional staff hiring and training and infrastructure upgrades, average USD 69,000 for large businesses and USD 8,000 for SMBs. ❖ Downtime, occurring in about one-third of security breach incidents, is the most expensive consequence, costing up to USD 1.4 million for large businesses. ❖ Damage to brand reputation, including consultancy expenses, lost opportunities, and marketing and PR activities, averages USD 8,653 for SMBs and USD 204,750 for enterprises.

The Economic Cost of Cybercrime *Grant Thorton* (2021)	
Summary	The report examines the financial impact of cybercrime on businesses in Ireland. The report finds that phishing attacks and ransomware are the most common types of cybercrime affecting Irish businesses. The report concludes that businesses need to invest in cybersecurity measures to protect themselves from cybersecurity threats and minimize the economic cost of cybercrime. The main contribution of this report is providing a clear estimate of the economic impact of cybercrime on Irish businesses and emphasizing the importance of cybersecurity measures.
Key highlights on the economic impacts of cybersecurity incidents	❖ In 2014, the cost of cybercrime in Ireland was EUR 630 million (USD 695 million), increasing dramatically to EUR 9.6 billion (USD 10.5 billion) in 2020. ❖ Cybercrime incidents in Ireland have been on the rise, with 61% of organizations falling victim to cybercrime such as fraud in the past two years, and average estimated losses of EUR 3.1 million (USD 3.4 million). ❖ Irish firms ranked joint third in cybersecurity spending among eight countries measured but had the largest proportion of cybersecurity novices (36%). Median costs for Irish firms were EUR 7,251(USD 8,000) compared to a range of EUR 8,736 (USD 9,643) to EUR 103,000 (USD 113,698) for organizations with 50-249 employees and EUR 21,000 (USD 23,181) to EUR 404,000 (USD 445,915) for larger organizations. ❖ The overall value of potential financial losses from cyberattacks, including stolen IP, lost customers, ransomware, and industrial espionage, may far exceed the initial investment in cybersecurity. ❖ Indirect losses from cyberattacks are difficult to quantify, and companies often underestimate the risk, leading to inadequate preparation. ❖ The Banking and Payments Federation Ireland (BPF) reported that Irish consumers lost over EUR 12 million (USD 13.2 million) to debit and credit card fraud in the first half of 2020.
Ransomware: The True Cost to Businesses *Cybereason* (2022)	
Summary	This is a comprehensive analysis of the global ransomware threat landscape, based on survey data and interviews with nearly 1,500 cybersecurity professionals from organizations with 700 or more employees n United States, United Kingdom, Germany, France, Japan, Italy, South Africa, United Arab Emirates, and Singapore. The report finds that ransomware attacks continue to be a major threat to businesses of all sizes. Of the organizations that reported losses from a ransomware attack, more than two-thirds (67%) said that their combined losses reached between USD 1 million and USD 10 million. The report also highlights the growing sophistication of ransomware attacks, with threat actors using new tactics such as double extortion, where they not only encrypt a victim's data but also threaten to publish it unless a ransom is paid. In addition, the report emphasizes the importance of adopting a proactive and comprehensive approach to cybersecurity, including regular employee training, threat hunting, and incident response planning, in order to mitigate the risk of ransomware attacks.
Key highlights on the economic impacts of cybersecurity incidents	❖ Losses from cybersecurity incidents varied, with 4% of organizations reporting losses between USD 25 million and USD 50 million, while others (67%) experienced losses ranging from USD 1 million to USD 10 million. ❖ Ransomware dominated the threat landscape in 2022, doubling the volume of attacks from 2021 and resulting in an estimated total cost exceeding USD 20 billion. ❖ Ransomware attacks led to significant business impacts such as revenue loss, reputational damage, workforce reductions, and business disruption for affected organizations. ❖ Short-term impacts from ransomware attacks included disruption of critical business processes, costs of incident response and mitigation, lost productivity, and ransom payments if organizations chose to comply. ❖ Longer-term impacts encompassed diminished revenue, brand and reputation damage, loss of key executives, employee layoffs, loss of customers and strategic partners, and in some cases, jeopardizing the business's overall viability.
Cybersecurity Report *CheckPoint – Software Technologies LTD* (2021)	

Summary	The report offers a comprehensive analysis of the state of cybersecurity in the United States. It indicates that cyber threats are on the rise, with 81% of surveyed organizations reporting at least one cybersecurity incident in the past year. Additionally, the report highlights the increasing sophistication of attacks targeting cybersecurity, with ransomware, phishing, and social engineering attacks becoming more prevalent. The report emphasizes the need for organizations to invest in proactive cybersecurity measures such as employee training, incident response planning, and network segmentation in order to mitigate the risk of cyberattacks. Finally, the report highlights the importance of collaboration between organizations, governments, and cybersecurity experts in order to address the growing cybersecurity threat.
Key highlights on the economic impacts of cybersecurity incidents	❖ In 2020, the average time to identify and contain a cybersecurity breach was 280 days, with an average cost of nearly USD 4 million in losses and remediation. Ransomware attacks increased, costing businesses globally an estimated USD 20 billion, up from USD 11.5 billion in 2019.
Cyber Claims Analysis Report *Willis Towers Watson* (2020)	
Summary	The report finds that the number of claims is increasing, with the average cost of a claim rising to USD 369,000 in 2019. The most common types of attacks reported were business email compromise (BEC), ransomware, and unauthorized access, with the healthcare and financial services sectors being the most targeted. The report highlights the importance of organizations adopting a comprehensive approach to cybersecurity, including risk management, employee training, and incident response planning, to mitigate the risk of cyberattacks and minimize the impact of any resulting breaches.
Key highlights on the economic impacts of cybersecurity incidents	nearly one in ten settled claims, first party losses and data breach losses both had a total cost exceeding USD 2.5 million, uding defense costs and other expenses. direct event cost per breached record is USD 7.95 on average, with the cost per record decreasing significantly when a higher ıber of records are breached due to economies of scale. average settled cybersecurity claim is USD 4.88 million, and while losses over USD 10 million only make up 5% of claims by me, they account for 95% of total costs. somware events increased significantly in 2019 due to their low investment, low risk, high reward nature, and the anonymity vided by cryptocurrency payments, which may lead to a continued rise in such attacks.
Cyber Security Insights Report Global Results *Norton* (2017)	
Summary	The report provides an in-depth analysis of global cybersecurity threats, revealing the extent of cybercrime and its impact on consumers. Drawing from an online survey of 21,549 individuals aged 18+ across 20 countries, the study's main contribution is its comprehensive assessment of cybercrime prevalence. The report underscores the urgent need for increased cybersecurity awareness and the adoption of protective measures by consumers worldwide.
Key highlights on the economic impacts of cybersecurity incidents	❖ Consumers worldwide lost USD 172 billion due to cybercrime. ❖ 53% of their global research data (an online survey of 21,549 individuals ages 18+ across 20 markets) of consumers either experienced cybercrime themselves or knew someone who had. ❖ On average, cybercrime victims globally spent nearly 24 hours (23.6 hours) or almost three full workdays dealing with the aftermath of the incident.
