DOI: https://doi.org/10.5281/zenodo.15005192

NEGATIVE CONSEQUENCES OF CYBERATTACKS IN THE DIGITAL ECONOMY

Majidova Mokhigul
Samarkand branch of the Tashkent State University of Economics
Scientific researcher
majidovamohigulshuxratovna@gmail.com

Abstract: *The negative consequences of cyberattacks in the digital economy are vast and multifaceted. They can cripple businesses financially, disrupt operations, destroy consumer trust, and undermine the overall security and growth of the digital landscape. Therefore, robust cybersecurity strategies and continuous investment in cyber resilience are crucial for mitigating these risks and sustaining the digital economy. Cyberattacks in the digital economy can lead to a wide range of losses, affecting businesses, governments, consumers, and society as a whole. These losses are not limited to direct financial damage but can also extend to reputational harm, legal consequences, operational disruptions, and long-term impacts on innovation and trust. Below are the major types of losses businesses and economies face from cyberattacks. The losses stemming from cyberattacks in the digital economy are vast and multifaceted. They encompass direct financial damage, reputational harm, operational disruptions, legal consequences, and broader economic and societal impacts. As cyberattacks become more frequent and sophisticated, businesses, governments, and individuals must prioritize cybersecurity to mitigate these risks and protect the growing digital infrastructure that underpins the global economy.*

Keywords: *operational disruption, financial losses, cybersecurity, cybercrime, virtual applications, web servers, cybercriminals, global economic impact.*

INTRODUCTION

Cyberattacks have significant negative consequences for the digital economy, impacting businesses, governments, and individuals across multiple dimensions. Here are some of the key negative consequences: Cyberattacks can lead to direct financial losses, including ransom payments (in the case of ransomware attacks), theft of sensitive financial data, or the cost of restoring compromised systems. Indirect Costs: Loss of business opportunities due to downtime, legal fees, and fines for data breaches can add up, causing financial strain. Companies may also lose intellectual property, trade secrets, or other assets that can harm their competitive position. Insurance Premiums: The increased risk of cyberattacks leads to higher cyber insurance premiums for businesses, further escalating costs. Cyberattacks, especially those that compromise customer data, erode consumer trust and damage a company's brand reputation. Customers may be hesitant to engage with a business that has suffered a breach, and negative publicity can have long-term effects on brand perception. A damaged reputation can result in customer churn and a loss of future revenue streams, particularly for companies operating in highly competitive markets. Cyberattacks can cause significant disruptions to business operations, leading to system outages, data loss, and delays in the production and delivery of goods and services. Recovery Time: After an attack, businesses must invest significant time and resources to recover data, fix vulnerabilities, and restore normal operations, causing prolonged interruptions. Impact on Supply Chains: Cyberattacks can also disrupt supply chains, affecting suppliers, distributors, and other partners, leading to broader economic implications. Cybercriminals may target organizations to steal sensitive data, intellectual property, and proprietary information. The theft of such assets can have long-term impacts on an organization's ability to innovate and compete. Competitors or other malicious actors might exploit stolen intellectual property, potentially leading to market imbalances and unfair competition. Organizations that experience data breaches may face legal action from customers, regulators, or business partners. In some cases, companies may face fines and penalties for non-compliance with data protection laws (e.g., GDPR, HIPAA,

etc.).Governments have started to impose stricter regulations on cybersecurity practices, meaning that failure to adhere to these laws can lead to even more significant financial and reputational costs. Cyberattacks undermine consumer confidence in digital platforms and services. People may be less willing to conduct online transactions or share personal information if they fear their data may be compromised. This reduction in consumer confidence can slow down the growth of the digital economy, as consumers retreat from online services and transactions in favor of traditional, more secure methods. SMEs, which may have fewer resources to devote to cybersecurity, are particularly vulnerable to cyberattacks. A breach or attack could be catastrophic for these businesses, potentially leading to bankruptcy. The increasing cost of cybersecurity for SMEs, as well as the potential loss of customer trust, can further hinder their ability to grow and compete in the digital economy. The constant threat of cyberattacks can stifle innovation, as businesses may focus more on defensive cybersecurity measures rather than new product development, research, and growth. Small startups or innovation-driven companies may be especially vulnerable, as they may not have the resources to implement robust cybersecurity systems, hindering their ability to scale effectively. Cyberattacks can target critical infrastructure, such as power grids, transportation systems, and government institutions, potentially leading to widespread chaos. This can impact a nation’s economy, safety, and security. State-sponsored cyberattacks can also be used for espionage, cyber warfare, or to manipulate political processes, leading to significant geopolitical tensions and instability. Cyberattacks often lead to an increase in cybercrime and the proliferation of malware, making the digital environment less secure. This perpetuates a cycle of cyber threats and further undermines trust in digital services. The cost of dealing with increasing levels of cybercrime, including the development of better detection systems and prevention methods, can drain resources from other sectors of the economy. In summary, the negative consequences of cyberattacks in the digital economy are vast and multifaceted. They can cripple businesses financially, disrupt operations, destroy consumer trust, and undermine the overall security and growth of the digital landscape.

Therefore, robust cybersecurity strategies and continuous investment in cyber resilience are crucial for mitigating these risks and sustaining the digital economy.

LITERATURE REVIEW

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. 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

DISCUSSION

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 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. By providing a detailed breakdown of the many different ways a cyber-attack can impact a business and third-parties, it gives board members and other senior staff a better understanding of both direct and indirect harms from cyber-attacks when considering the threats their organisation faces. This also equally applies to other organisations and even governments or those who manage critical national infrastructure. Commenting on the article, Dr Jason R.C. Nurse from the School of Computing: ‘It’s been well understood that cyber-attacks can have numerous negative impacts. However, this is the first time there has been a detailed investigation into what these impacts are, how varied they can be, and how they can propagate over time. This base figure of 57 underlines how

damaging cyber-incidents can be and we hope it can help to better understand how a business, individual or even nation is affected by a cyber-attack. This is going to be even more relevant as everything and everyone becomes connected and the Internet of Things is fully realised.

RESULTS

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. Summary The IBM report on data breaches examines the impact and cost of data breaches on organizations using data from real-worldincidents—excluding very small and very large data breaches to avoid the results to be skewed. Data breaches examined in the2022 version ranged in size between 2,200 and 102,000 compromised records. In-depth qualitative also comprised of over 3,600separate interviews with staff at 550 organizations between 2021 and 2022. The report identifies key factors that influence thecost of data breaches, including the size of the breach, the time it takes to identify and contain the breach, and the use of certainsecurity measures. The study also highlights the importance of incident response planning and the need for organizations toprioritize their security investments. In conclusion, the report emphasizes the critical need for organizations to invest inproactive security measures and comprehensive incident response plans to mitigate the impact and cost of data breaches. 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 tothe 2021 findings, with Brazil having the largest relative

cost increase (27.8%, from USD 1.08 million toUSD 1.38 million) and Türkiye experiencing the biggest cost decrease (42%, from USD 1.91 million toUSD 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 toUSD 4.54 million in 2022. However, the occurrence of ransomware breaches has increased by 11% in the 2022 study compared tothe 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 toorganizations 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). The reportidentifies the increasing frequency and sophistication of cyberattacks as a major threat to global economic growth and the digitalecosystem. 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 takeproactive steps to secure the digital economy and protect the privacy and trust of users.

REFERENCES

1. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2020 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry " by G.Nikhita Reddy, G.J.Ugander Reddy

2. Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause. IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2021.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

3. 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%20Cy ber%20Power%20Index%202022_v3_220922.pdf

4. 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.

5. 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.

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

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

8. 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.

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