International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

Study on the Recent Cyber Security-Attacks and the Economic Loss Due to the Growing of Cyber-Attacks

Dr. Abhilash Maroju,

Ph.D. Research Graduate, Department of Information Technology, University of the Cumberlands , USA.
doctorabhilashmaroju@gmail.com

Dr. Srinivas A Vaddadi,

PhD Research Graduate, Department of Information Technology, University of the Cumberlands , USA. Vsad93@gmail.com

Dr. Rohith Vallabhaneni,

PhD Research Graduate, Department of Information Technology, University of the Cumberlands , USA.
rohit.vallabhaneni.2222@gmail.com

Sravanthi Dontu,

PhD Research Student, Department of Information Technology, University of the Cumberlands, USA.
sravanthi.dontu13@gmail.com

ABSTRACT

Economic damages caused by cyberattacks have been on the rise recently, on a global scale. However, there has not been enough research on the economic damage caused by cyberattacks to other industries; most studies have concentrated on the attacked enterprises. As a means of better damage prediction and other national measures, this study examined the economic damages inflicted on Japan by cyberattacks by employing the production function and the input-output model. We begin by outlining a production function–based approach to estimating the yearly direct harm by industry. Working hours lost due to cyber events are the major input dataset. Second, we used the input-output model to create a model that could estimate the national spillover damage. Thirdly, we explained how to estimate direct and spillover harm in all Japanese industries, even if the data on cyber damage was confined to interview data from the JNSA and the IPA. Therefore, we think our approach of estimating is workable and efficient on a nationwide scale.

1. INTRODUCTION

Organisations face cyber threats as a result of society's shift to a knowledge-based economy, our growing reliance on the IT industry, and the pervasiveness of digital technologies in nearly every aspect of life. The WannaCry ransomware attack of 2017 damaged healthcare institutions and numerous other organisations worldwide, causing economic damages estimated at $8 billion [1]. This incident exemplifies the potential for severe effects. According to estimates, the annual economic consequences of cybercrime will reach around $1 billion in 2020, up from $600 billion in 2018 [2]. The relevance of cyber hazards to the economy has been magnified due to COVID-19 and the post-pandemic world's rising reliance on digital technologies ([3]). Cost estimates for cyber risk (which includes much more than cybercrime) are scarce and differ greatly between research since historical data is not readily available, which is partly because there are disincentives for reporting and revealing cyber incidents. In addition, past incidents are not always indicative of future occurrences, and the inherent variability and multidisciplinary study environment of cyber hazards restrict the use of historical data for cyber risk analysis [4].

Several scenarios have been suggested in industry research and applied literature as alternatives to bring more attention to the issue among executives, the public, media, and lawmakers [5]. In the worst-case situation, essential infrastructure is disrupted, leading to economic losses. The possible accumulation of losses in the event of a cyber catastrophe is a well-discussed feature in this context, and it is related to the monocultures in the soft- and hardware markets [6].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

The predicted monetary impacts of the scenarios exhibit a wide range of values, from 0.2 percent to 2 percent of GDP in the event year. The studies do not share any common methods, aims, or themes, hence it is difficult to compare the scenarios or do a thorough economic effect analysis ([7]). Managers and lawmakers are thus left with an imprecise understanding of the frequency and seriousness of extreme cyber hazards, which in turn leads to imprecise risk management techniques.

We create a system that can consistently analyse the economic impact of various cyber risk scenarios. This is accomplished by sorting through the particular features of six commonly debated cyber risk scenarios and reviewing and evaluating them. Next, we provide a standardised approach for measuring economic losses caused by cyber hazards. This framework can be used to evaluate the costs of past and future occurrences, and it can be applied at both macroeconomic and microbusiness levels. This paves the path for organisations to gauge the best use of their information security budget in a consistent and repeatable manner. Consistent analysis of the economic impact of different cyber risk scenarios provided in the applied literature has not been attempted before, as far as we are aware [8].

2. LITERATURE REVIEW

Cybercrime has become more common and more severe as a result of globalisation, digitization, and smart technologies. Cybersecurity is still a relatively new area of study and business, but companies, governments, and international organisations have all begun to recognise the need for strong cybersecurity protection systems. It is projected that the global economy lost USD 945 billion in 2020 due to insufficient cybersecurity [9]. Risks to corporations from cyber vulnerabilities include disruptions to operations, invasions of privacy, and monetary losses. Cyber dangers are becoming more important to the global economy, yet there is still a lack of data on them. There are a lot of causes behind this. First, there is a lack of historical data sources because the danger is new and changing [10]. The fact that most compromised organisations choose to keep quiet about the hacks could also be a contributing factor [11]. Many domains, including cybersecurity, risk management, and research, face difficulties due to a lack of data [12]. The announcement made by the European Council in April 2021 on the establishment of a cybersecurity centre to consolidate investments in R&D, technology, and industrial development highlights the topic's significance. Improving the safety of the web and other vital data networks is the primary objective of this facility [13].

From a risk management vantage point, this study examines cyber risk, cyber insurance, and cybersecurity as tools for transferring and mitigating this type of risk. Cybersecurity and cyber risk are the topics of this study, which scours the current literature and public data sources for relevant information. When considering cyber risk and cybersecurity generally, this is the first comprehensive study of data availability.

Supporting the scientific community, this work identifies and critically analyses all available open datasets, then aggregates, summarises, and categorises them. Stakeholders involved in cyber risk control and cybersecurity can benefit from the additional information on datasets that is attached, which will provide deeper insights. The last point made in this study is the importance of having free and unfettered access to cyber-specific data [14].

Cyber insurers might use the found accessible data to aid in the development of sustainable products. Because of a lack of claims data from the past, insurance companies have been unable to use traditional risk assessment procedures. Because there is a lot of room for speculation, cyber insurers are likely to charge too much for cyber risk coverage [15-17]. In order to improve the risk evaluation and achieve risk-adjusted pricing, it appears that combining external data with insurance portfolio data is crucial.

3. METHODOLOGY

3.1. Leontief Input–Output Model

National and regional economies are described by the Leontief input-output model in its equilibrium behaviour. Modern input-output analysis has many more uses than its first one, which was to measure the magnitude of economic changes (such as changes in consumption). Because the economy is made up of so many interconnected parts, the input-output model is useful for studying how these parts react to disturbances. Interdependencies occur when one industry relies on input factors supplied by another. Household consumption and international trade (import and export) are also accounted for in the model. Here is the fundamental role of the initial input-output model:

$$\boldsymbol{x} = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{c} \Leftrightarrow \left\{ x_i = \sum_j a_{ij} x_j + c_i \right\} \forall i.$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

3.2. Inoperability Input–Output Model

Haimes and Jiang's classic Leontief input-output model was expanded upon in the demand-based input-output inoperability model. As deterministic linear equilibrium models, the inoperability and classic Leontief input-output models share a common data set. Having said that, a number of distinctions exist on a theoretical and practical level. The inoperability input-output model utilises an interdependency matrix rather than the technical coefficient matrix.

$$q = A^* q + c^* = \left[I - A^*\right]^{-1} c^*$$

4. CYBER RISK SCENARIOS

Cyberattacks on diverse industries can originate from different places and have varying degrees of complexity. Earthquakes and floods are examples of natural disasters that can create (physical) IT interruptions, however the majority of dangers are actually produced by humans.

Attackers, whether state-sponsored, criminals, hackers, or terrorists, can have ideological, financial, political, or religious motives when they launch cyberattacks. Malware, insider assaults, spam, DDoS, and physical damage to IT systems are the various forms of cyberattacks (Eling and Schnell 2016). By crafting emotionally engaging narratives, cyber risk scenarios paint the worst-case scenario of a cyberattack. To address the most pressing concerns about cyberattacks, we have compiled a list of six cyber risk scenarios:

1. A data acquisition and supervisory control network extortion.
2. The collapse of a cloud provider.
3. A cyberattack on the health industry and hospitals.
4. Municipal services are being compromised.
5. A problem with online communication.
6. An IT failure that spans sectors

5. RESULTS AND STUDY

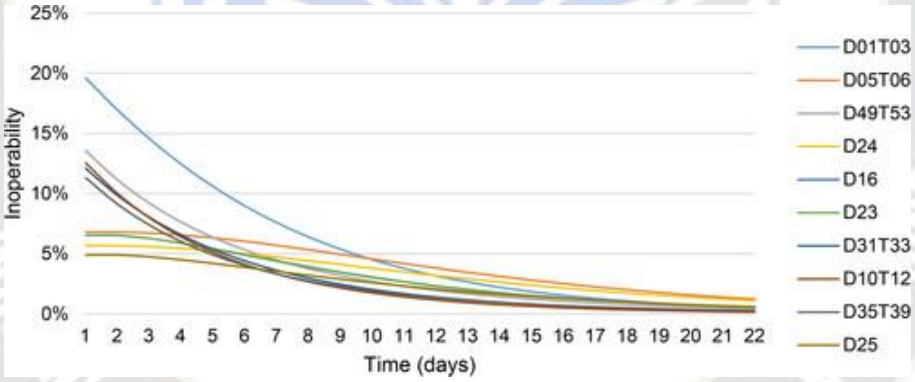

FIGURE 1. Inoperability Development of the Top 10 Inoperable Sectors.

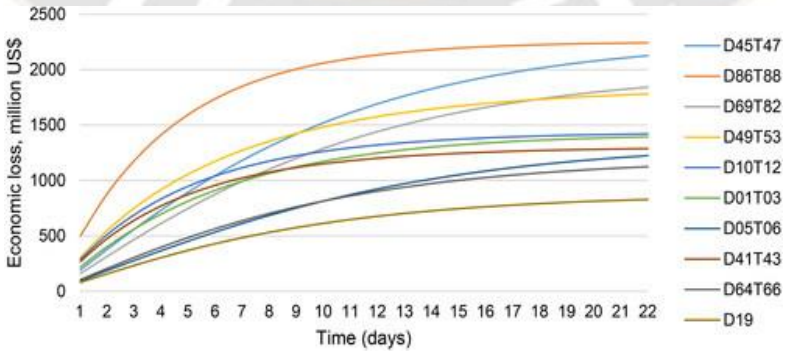

FIGURE 2. Cumulative Economic Losses for the Top 10 Affected Sectors.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

Figure 2 shows the total economic loss for the top ten impacted sectors and Figure 1 shows the growth of the inoperability.

CONCLUSIONS

In terms of economic loss and inoperability, this article evaluates six commonly mentioned cyberattack scenarios. We reliably evaluate the economic damages of several cyber risk scenarios, including ripple effects, using the dynamic input-output model tool. One way to find out how sensitive the inoperability rankings are to various input parameters is to use fuzzy values. A comprehensive view, as well as comparability and scalability for future research, are made possible by combining the qualitative classification of cyber risk scenarios using a standardised taxonomy with the quantitative estimate of economic losses. In all of our six popular cyber risk scenarios, the possible economic losses are within the insurable range, and they vary from $0.7 billion to $35 billion. Crucially, the article's primary conclusion does not centre on the exact monetary amounts. Economic impact models typically fail to account for the substantial role played by qualitative context in such analyses, at least in the cyber realm. Our findings can help policymakers and decision-makers qualitatively determine how new scenarios they face align with our scenario framework, allowing them to estimate the economic impact in rough terms of magnitude. They can also use this information to determine if market-intervening tools, such as government backstops, are necessary.

REFERENCES

1. Direct costs include the costs borne directly by the sector(s) targeted by the cyberattack (e.g., business interruptions, litigation costs, and fines), while systemic costs comprise the macroeconomic impact on productivity experienced by the nonaffected sectors due to the direct damage in the sector(s) affected by the cyberattack (Dreyer et al. Citation2018).
2. They found that cybercrime results in total costs of US$799 billion to 22.5 trillion (1.1 to 32.4 percent of global GDP). In additional material available upon request we also include a solar storm, but we excluded it from the analysis presented in the main body of this article because it is caused by a natural geophysical phenomenon.
3. See Jin et al. (2018) for an application of an econometric model to evaluate the loss due to surge disasters in China.
4. See Feenstra and Sasahara (2018) for a quantification of the impact on U.S. employment from imports and exports between 1995 and 2011, applying input–output analysis.
5. See Kajitani and Tatano (2018) for a recent discussion about the applicability of the computable general equilibrium model to assess short-term economic impacts of natural disasters. Computable general equilibrium models are also referred to as applied general equilibrium models (Ballard and Johnson 2017).
6. See Leontief (Citation1951; Citation1966; Citation1974). A comprehensive introduction to the model and its applications is provided by Miller and Blair (Citation2009).
7. Inoperability is defined as the deviation of the actual activity level from the planned operation level (Niknejad and Petrovic Citation2016).
8. Jung et al. (Citation2009).
9. Aamir, M., S.S.H. Rizvi, M.A. Hashmani, M. Zubair, and J. Ahmad. 2021. Machine learning classification of port scanning and DDoS attacks: A comparative analysis. *Mehran University Research Journal of Engineering and Technology* 40 (1): 215–229. https://doi.org/10.22581/muet1982.2101.19.
Article Google Scholar
10. Aamir, M., and S.M.A. Zaidi. 2019. DDoS attack detection with feature engineering and machine learning: The framework and performance evaluation. *International Journal of Information Security* 18 (6): 761–785. https://doi.org/10.1007/s10207-019-00434-1.
11. Barzegar, M., and M. Shajari. 2018. Attack scenario reconstruction using intrusion semantics. *Expert Systems with Applications* 108: 119–133.
12. Chatterjee, S., and S. Thekdi. 2020. An iterative learning and inference approach to managing dynamic cyber vulnerabilities of complex systems. *Reliability Engineering and System Safety*. https://doi.org/10.1016/j.ress.2019.106664.
13. De Giovanni, A.L.D., and M. Pirra. 2020. On the determinants of data breaches: A cointegration analysis. *Decisions in Economics and Finance*.
14. Eling, M., and K. Jung. 2018. Copula approaches for modeling cross-sectional dependence of data breach losses. *Insurance Mathematics & Economics* 82: 167–180.
15. Eling, M., and J. Wirfs. 2019. What are the actual costs of cyber risk events? *European Journal of Operational Research* 272 (3): 1109–1119.
16. Ramya Manikyam, J. Todd McDonald, William R. Mahoney, Todd R. Andel, and Samuel H. Russ. 2016.Comparing the effectiveness of commercial

obfuscators against MATE attacks. In Proceedings of the 6th Workshop on Software Security, Protection, and Reverse Engineering (SSPREW'16)

17. R. Manikyam. 2019.Program protection using software based hardware abstraction.Ph.D. Dissertation.University of South Alabama