EasyChair Preprint

№ 15245

# Cyberattacks: Economic Impacts and Risk Management Strategies

Friederikos Fotis



October 18, 2024

# Cyberattacks: Economic Impacts and Risk Management Strategies

Friederikos Fotis

*Faculty of Management, Comenius University, 820 05 Bratislava, Slovakia*
*E-mail address: rico@fotis.de*
*ORCID-ID: 0000-0001-9918-3545*

**Abstract**

The widespread adoption of emerging information and communication networks has increased organizations' vulnerability to cyberattacks. These attacks – including data breaches, ransomware, and other cyber threats – pose significant economic risks to the stability of modern businesses. This study offers a comprehensive analysis of the economic impacts of cyberattacks within the context of these emerging networks and outlines effective cyber risk management strategies to enhance organizational resilience. The research elucidates the complex economic repercussions of cyber threats by conducting a rigorous literature review and an in-depth case study of the 2019 ransomware attack on Norsk Hydro ASA. The findings underscore the critical necessity for robust cybersecurity measures in the evolving digital landscape.

*Keywords: Cyber Security; Cyber Threats; Cyber Attacks; Cyber Risk Management; Cyber Risk Strategies; Cyber Resilience; Economic Impact;*

## 1. Introduction

Emerging information and communication networks have revolutionized business operations, fostering unprecedented connectivity and data exchange. However, this increased interconnectedness has also escalated organizations' vulnerability to cyberattacks—malicious activities exploiting weaknesses in digital infrastructures. Cyberattacks such as data breaches, ransomware, and denial-of-service attacks can disrupt operations, tarnish reputations, and inflict substantial economic losses [10] [9].

As organizations integrate advanced networking technologies, cyber threats' complexity and potential financial damages intensify. The economic repercussions encompass direct costs like system restoration and legal penalties and indirect effects such as diminished customer trust and market share erosion [3]. While offering operational benefits, the integration of emerging networks also introduces novel security challenges that necessitate sophisticated risk management strategies.

This study aims to:

- Analyze the primary economic effects of cyberattacks on organizations within emerging networks.
- Examine how organizations across various industries and sizes experience and respond to cyber threats.
- Identify effective cyber risk management strategies tailored to the challenges posed by emerging information and communication networks.

This paper's structure includes a review of relevant literature on the economic impacts of cyberattacks and cyber risk management strategies, a methodology outlining the research design, a presentation of findings from the empirical analysis, and a discussion summarizing key insights with implications for practice.

## 2. Theoretical Background

### *2.1. Economic Impact of Cyberattacks on Emerging Networks*

Integrating emerging information and communication networks enhances operational efficiency but concurrently amplifies cyber risks. Cyberattacks exploit vulnerabilities inherent in advanced networking technologies, leading to significant economic consequences. Direct economic impacts involve immediate costs such as IT system recovery, legal fees, and regulatory fines [15]. According to IBM Security [9], the global average data breach cost has reached $4.45 million, reflecting the escalating financial stakes.

Indirect impacts are pervasive and enduring, affecting customer trust, brand reputation, and market positioning [4]. Loss of customer confidence can precipitate revenue declines, while reputational damage may have long-term adverse effects on organizational viability. Furthermore, cyberattacks can disrupt supply chains [1] and stifle innovation, particularly within organizations heavily reliant on emerging networks [7].

### *2.2. Cyber Risk Management Strategies for Emerging Networks*

Effective cyber risk management is imperative to mitigate the economic damages associated with cyber threats in emerging networks. Strategies encompass preventive measures, incident response planning, and continuous improvement.

Preventive Measures: Implementing advanced security protocols, such as next-generation firewalls and intrusion detection systems, is critical. Regular security assessments and employee training on cybersecurity awareness are essential to preempt potential attacks [13]. Organizations investing in proactive security measures can reduce the risk of successful cyberattacks by up to 70%.

Incident Response Planning: Developing a robust incident response plan tailored to the complexities of emerging networks ensures rapid identification, containment, and remediation of cyber incidents [14]. Effective response strategies minimize downtime and financial losses, maintaining operational continuity.

Continuous Improvement: The dynamic nature of cyber threats necessitates ongoing evaluation and enhancement of security measures. Adapting to new vulnerabilities emerging networks introduce requires organizations to stay abreast of technological advancements and threat intelligence [19].

### *2.3. Significance for Organizations*

Integrating comprehensive cyber risk management into corporate governance is essential for organizations leveraging emerging information and communication networks. Such integration ensures that cybersecurity considerations are aligned with strategic objectives, fostering resilience and competitive advantage [7].

## 3. Methodology

### *3.1. Research Design*

This study follows a dual approach, combining a thorough literature review with a case study on Norsk Hydro ASA. The literature search includes scientific publications, current research articles, scientific papers, and so-called grey literature. Grey literature refers to materials and research not published through traditional publishers, such as reports from government agencies, research institutes, NGOs, and companies [11]. These sources are particularly valuable in the field of cybersecurity, as they often contain up-to-date and practice-relevant information that may not be available in scientific journals [2]. The collected sources were qualitatively evaluated according to relevance, quality, topicality, and content as part of the literature research. The focus was on central topics, concepts, and models, as well as analysis of the effects of cyberattacks on different industries and company sizes and the effectiveness of various risk management strategies. The case study includes an investigation into the 2019 cyberattack on Norsk Hydro ASA using data from interviews and statements from Norsk Hydro executives and IT security officers, official press releases, and reports from Norsk Hydro and IT security companies that analyzed the incident [5] [16] as well as media reports and analyses [12] [18] industry analysis and reports on the impact of ransomware attacks [6].

### *3.2. Data Collection and Analysis*

The qualitative data collected from the literature review and the results of the case studies were evaluated through thematic analysis to identify patterns and insights related to cybersecurity and risk management. By combining the literature review and a practice-oriented case study, this study pursues a methodological approach that sheds light on both theoretical and practical aspects of the economic impact of cyberattacks and the effectiveness of cyber risk management strategies. This methodology ensures that the insights gained are well-founded and relevant to practice, leading to a deeper insight into the topic and providing companies with concrete recommendations for action.

Data were collected from authoritative sources, including academic databases and official reports from cybersecurity organizations. The case study focuses on the 2019 ransomware attack on Norsk Hydro ASA, utilizing information from company reports, expert analyses, and media coverage [8] [5].

Thematic analysis was conducted to identify patterns and extract insights about the economic impacts and effectiveness of cyber risk management strategies in emerging networks.

## 4. Results

### *4.1. Economic Effects of Cyber Attacks*

Organizations affected by cyberattacks incur substantial immediate costs, including expenses related to system restoration, legal actions, and compliance fines. Direct financial losses are significant, with ransomware attacks resulting in average costs of $1.85 million per incident [17]. Additionally, cyberattacks lead to significant operational downtime, with organizations experiencing an average of 22 days of disruption, adversely affecting productivity and revenue streams [6]. Beyond these immediate impacts, there are long-term repercussions on brand reputation, leading to customer attrition and loss of market share. Affected organizations reported a 10% decline in customer base within a year post-attack [15].

### *4.2. Effectiveness of Cyber Risk Management Strategies*

Proactive security measures have proven highly effective in reducing the impact of cyber threats on organizations. Investment in advanced cybersecurity technologies and continuous employee training has resulted in a 50% reduction in successful cyberattacks [13]. Moreover, organizations with established incident response protocols have experienced a 35% reduction in recovery time and a 25% decrease in financial losses [14]. Cyber insurance further mitigates financial impacts, with organizations reporting 40% lower out-of-pocket expenses and gaining access to specialized response services [10]. Incorporating cybersecurity into corporate governance structures enhances organizational resilience, reducing the frequency and severity of attacks by 30% [19].

## 5. Case Study: Norsk Hydro ASA Cyberattack

In March 2019, Norsk Hydro ASA, a global aluminum producer, suffered a significant cyberattack from the LockerGoga ransomware. The attack crippled IT systems and disrupted production across facilities in 40 countries [8].

### *5.1. Economic Impact*

The cyberattack resulted in significant production losses for Norsk Hydro ASA, with estimated losses ranging from $40 million to $50 million due to halted operations across multiple facilities. The company faced substantial recovery costs, incurring significant expenditures to restore its IT infrastructure and enhance security measures. Additionally, the incident led to a decline in shareholder confidence and a decrease in market value, reflecting the reputational damage suffered by the organization.

### *5.2. Response and Mitigation*

Norsk Hydro refused to pay the ransom and collaborated with cybersecurity experts to restore systems. The organization implemented enhanced security protocols, conducted employee training, and integrated cyber risk management into corporate governance [5].

## 6. Discussion

### *6.1. Key Findings*

The study underscores the critical economic risks cyberattacks pose in emerging information and communication networks. Effective cyber risk management strategies are essential to mitigate these risks. The Norsk Hydro case exemplifies the profound impact of cyber threats and the importance of a resilient and strategic response.

### *6.2. Implications for Practice*

Organizations should invest in advanced cybersecurity technologies and continuously educate their employees to enhance their ability to prevent and respond to cyber threats. Developing and regularly updating incident response plans is crucial for ensuring preparedness and minimizing the impact of potential cyberattacks. Additionally, organizations should consider cyber insurance as a component of their risk management strategy to provide financial protection and access to specialized response services. Integrating cybersecurity into corporate governance is essential to align security measures with organizational objectives, fostering a culture of resilience and strategic risk management.

### *6.3. Conclusion*

The escalating integration of emerging information and communication networks necessitates a proactive and comprehensive approach to cybersecurity. By understanding the economic impacts of cyberattacks and implementing effective risk management strategies, organizations can enhance their resilience, protect their economic interests, and maintain competitive advantage in the digital era.

The results of this study show that cyberattacks can have a significant direct and indirect economic impact on companies. However, by implementing comprehensive cyber risk management strategies that include preventive, reactive, and continuous measures, organizations can increase their resilience to such attacks and minimize the economic consequences. The Norsk Hydro ASA case study illustrates the importance of being prepared for cyberattacks and responding quickly and effectively to such incidents. Norsk Hydro's experience and the literature sources analyzed provide valuable insights and practical recommendations for other companies looking to improve their cybersecurity strategies. To understand the diverse business impacts and associated technologies comprehensively, future research must identify gaps in the literature, recognize emerging trends, and pinpoint areas where further in-depth studies can significantly contribute to the field.

The following topics highlight key areas to enhance the outlook for future research:

Sector-Specific Impacts: Investigating the economic impacts of cyber-attacks on different sectors to develop tailored risk management strategies.

Long-Term Economic Effects: Studying the long-term economic effects of cyber-attacks on companies to understand the full extent of their impact.

Effectiveness of Emerging Technologies: Evaluating the effectiveness of emerging technologies, such as artificial intelligence and machine learning, in enhancing cybersecurity.

Global Cybersecurity Policies: Analyzing the impact of global cybersecurity policies and regulations on corporate cyber risk management practices.

By addressing these areas, future research can provide deeper insights into the dynamic landscape of cyber threats and help develop more effective strategies for mitigating their economic impacts.

## References

[1] Accenture. (2019). NINTH ANNUAL COST OF CYBERCRIME STUDY. https://iapp.org/resources/article/the-cost-of-cybercrime-annual-study-by-accenture/

[2] Adams, R. J., Smart, P., & Huff, A. S. (2017). Shades of Grey: Guidelines for Working with the Grey Literature in Systematic Reviews for Management and Organizational Studies. International Journal of Management Reviews, 19(4), 432–454. https://doi.org/10.1111/ijmr.12102

[3] Anderson, R., Barton, C., Bohme, R., Clayton, R., Gañán, C., Grasso, T., Levi, M., Moore, T., & Vasek, M. (2019). Measuring the changing cost of cybercrime.

[4] Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the Cost of

Cybercrime. In R. Böhme (Ed.), The Economics of Information Security and Privacy (pp. 265–300). Springer. https://doi.org/10.1007/978-3-642-39498-0_12

[5] Briggs, B. (2019, December 16). Hackers hit Norsk Hydro with ransomware. The company responded with transparency. Hackers Hit Norsk Hydro with Ransomware. The Company Responded with Transparency. https://news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

[6] ENISA. (2023, October). ENISA Threat Landscape 2023 [Report/Study]. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[7] European Central Bank. (2018). Cyber resilience oversight expectations for financial market infrastructures.

[8] Hydro. (2024, May 15). Cyber-attack on Hydro. https://www.hydro.com/en/global/media/on-the-agenda/cyber-attack/

[9] IBM Security. (2023). Cost of a Data Breach Report 2023. https://www.ibm.com/reports/data-breach

[10] Kshetri, N. (2018). The Economics of Cyber-Insurance. IT Professional, 20(6), 9–14. https://doi.org/10.1109/MITP.2018.2874210

[11] Lawrence, A., Houghton, J., & Thomas, J. (2014). Where is the evidence: Realising the value of grey literature for public policy and practice. Swinburne Institute for Social Research. https://doi.org/10.4225/50/5580B1E02DAF9

[12] Marks, G. (2019, April 11). Owners must protect their businesses from ransomware before it's too late. The Guardian. https://www.theguardian.com/business/2019/apr/11/small-business-ransomware-attacks-precautions-prevent

[13] McKinsey & Company. (2021). Cybersecurity in a digital era | Risk & Resilience | McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity-in-a-digital-era

[14] PricewaterhouseCoopers. (2021). 2021 Global Digital Trust Insights. PwC. https://www.pwc.com/kz/en/services/global-digital-trust-insights.html

[15] proofpoint. (2022). 2022 Ponemon Cost of Insider Threats Global Report. Proofpoint. https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats

[16] Slowik, J. (2020). SPYWARE STEALER LOCKER WIPER: LOCKERGOGA REVISITED.

[17] SOPHOS. (2021). The State of Ransomware 2021. https://assets.sophos.com/X24WTUEQ/at/k4qjqs73jk9256hffhqsmf/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469

[18] Tidy, J. (2019, June 25). How a ransomware attack cost one firm £45m. How a Ransomware Attack Cost One Firm £45m. https://www.bbc.com/news/business-48661152

[19] World Economic Forum. (2020). Global Risk Report 2020. https://www.weforum.org/publications/the-global-risks-report-2020/