EasyChair Preprint

№ 15244

Economic Impact of Cyber Attacks and Effective Cyber Risk Management Strategies: a Light Literature Review and Case Study Analysis

Friederikos Fotis

October 18, 2024

Economic Impact of Cyber Attacks and Effective Cyber Risk Management Strategies: A light literature review and case study analysis

Friederikos Fotis

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

Abstract

Businesses increasingly rely on digital technologies in the digital age, making them vulnerable to cyberattacks. These attacks, which range from data leaks to ransomware, can cause significant economic damage. Effective cyber risk management strategies that include preventive, reactive, and continuous measures can significantly reduce the risk and impact of such attacks. Norsk Hydro's case study illustrates the importance of a robust incident response plan and continuous improvements in cybersecurity measures. This study examines the economic impact of cyberattacks on organizations and identifies effective cyber risk management strategies that can strengthen organizational resilience. The methodology is based on a light literature review, including scientific and grey literature. It also includes an analysis of a real-world case study: the ransomware attack on Norsk Hydro ASA in 2019. The results show that cyberattacks cause direct costs. Furthermore, this study contributes to the academic discourse on cybersecurity and economic resilience by providing evidence-based insights and practical recommendations for businesses. Companies that invest in comprehensive cyber risk management strategies can ensure economic stability and gain competitive advantage by better managing the complexities of the digital landscape.

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

1. Introduction

In the digital age, companies heavily rely on digital technologies, exposing them to potential cyberattacks - digital assaults exploiting vulnerabilities in their systems. Cyberattacks, such as data breaches, code injection, ransomware, phishing, or denial-of-service attacks, can disrupt operations, damage a company's reputation, and cause significant economic losses [9][10]. As digital integration deepens, the potential financial damage from cyberattacks escalates.

The economic repercussions of cyberattacks are multifaceted, encompassing direct costs like repairing or replacing IT equipment, legal fees, and fines [15], as well as indirect effects such as loss of customer trust, reduced brand value, and decreased market share [4]. Additionally, cyberattacks can disrupt supply chains, hinder innovation, and create barriers to market entry, further amplifying the economic impact [7]. Damage severity ranges from negligible to existential threats, making cybersecurity—protective mechanisms against cyberattacks—critical for businesses of all sizes and industries [7]. Despite increased awareness, many organizations remain ill-prepared for effective cyber risk management due to a limited understanding of evolving threats, insufficient investment in cybersecurity measures, and inadequate integration of cyber risk management into corporate governance [19]. Consequently, the urgent need for robust cyber risk management strategies to reduce incident likelihood and mitigate potential impacts is more pronounced than ever [14].

This article provides a comprehensive understanding of the economic impact of cyberattacks on companies and identifies effective cyber risk management strategies to enhance organizational resilience. Through a thorough literature review and an in-depth analysis of a real-world example, this study equips readers with insights into how cyberattacks affect business performance and what risk strategies can be adopted for protection.

This paper addresses the following research questions:

- What are the main economic effects of cyberattacks on companies?
- How do companies of different industries and sizes experience and react to cyber threats?
- What are the most effective strategies for managing cyber risks and mitigating their economic impact?

The article is structured as follows to answer these questions: The theoretical background reviews current literature on the economic impact of cyberattacks and cyber risk management strategies. The methodology outlines the research design, data collection, and analysis methods used in the study. The results present findings from the empirical analysis, highlighting the main economic effects of cyberattacks and the effectiveness of different cyber risk management strategies. Finally, key findings are summarized, practical implications are discussed, and future research activities are proposed. This study contributes to the academic discourse on cybersecurity and economic resilience by providing evidence-based insights and practical recommendations for businesses. Understanding the economic impact of cyberattacks and identifying effective risk mitigation strategies equips organizations to manage the digital landscape's complexity better and protect their economic interests.

2. Theoretical Background

2.1. Material

2.1.1. Economic impact of cyberattacks

Companies' increasing digitization and networking offer opportunities but are also associated with considerable risks. Cyberattacks have become one of the biggest threats to companies' economic stability and security. These attacks can result in significant financial losses, including direct and indirect effects. Direct economic impacts include the immediate costs incurred by a cyberattack. These include IT system recovery costs, legal expenses, fines, and compensation for affected customers [15]. According to a study by IBM conducted by the Ponemon Institute in 2023

[9], the average cost of a data breach worldwide reached an all-time high of $4.45 million. This represents a 2.25% increase from the 2022 study, when the average cost was $4.35 million.

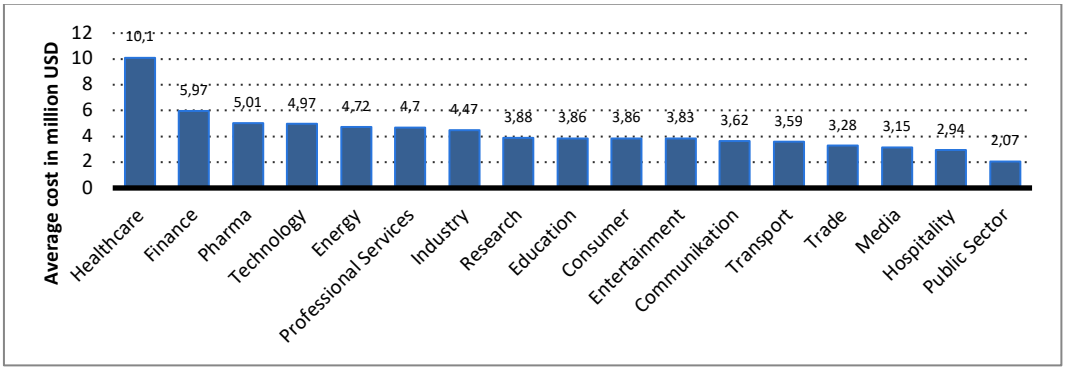

Fig. 1. Average Cost of Data Leaks Globally by Industry in 2022. Source: Statista; IBM; Ponemon Institute.

Indirect economic impacts are often long-term and affect a company's trust, image, market value, and market position. A loss of customer trust can lead to a decline in sales, while damage to the company's image can have an equally lasting impact [3]. In addition, cyberattacks can hinder innovation processes and lead to disruptions in the supply chain, causing additional costs and economic uncertainties [7]. Figure 2 shows a global study by Hiscox conducted by Forrester Research from 2021 to 2023 that found that the average cost of a single cyberattack is significantly high by country. The study also shows that the costs develop greatly over time from country to country, which could indicate the respective cyber risk strategies, among other things.

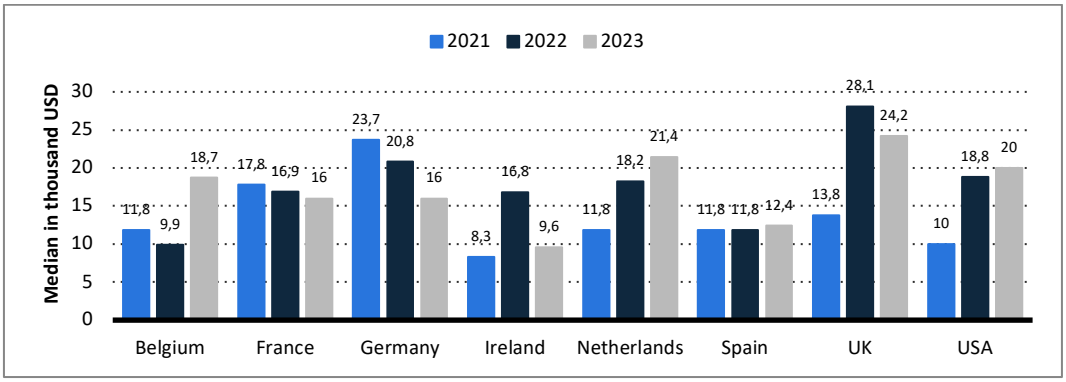

Fig. 2. Average cost of a cyberattack by country in 2023. Source: Hiscox.

2.1.2. Cyber Risk Management Strategies

Effective cyber risk management is essential to minimize the economic damage of cyber-attacks. This includes several strategies and measures to reduce the likelihood of cyber incidents and limit their potential impact. Preventive measures are designed to prevent cyberattacks before they occur. This includes regular security reviews, implementation of advanced security technologies such as firewalls and intrusion detection systems, and training of employees to deal with cyber threats. Companies that invest in preventative security measures can reduce the risk of a successful cyberattack by up to 70%.

Figure 3 shows a global survey by PricewaterhouseCoopers in 2024 on the estimated cost of the most consequential data breach in the last three years for businesses.

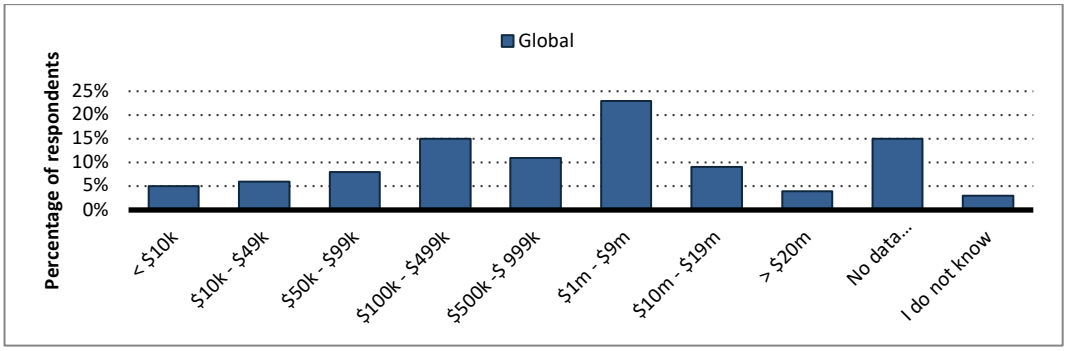

Fig. 3. Survey: Estimated Cost of Data Breaches in Enterprises in 2024. Source: PricewaterhouseCoopers.

Reactive measures concern the response to cyberattacks as soon as they are discovered. An effective incident response plan is critical to combating a current cyberattack, minimizing the extent of damage, and ensuring business continuity. This plan should include pre-developed risk scenarios for identifying, containing, and remedying security incidents and communication with stakeholders [6]. Continuous improvement is another important aspect of cyber risk management. This includes regularly reviewing and updating security strategies and technologies and adapting to new threats and technological developments [14]. According to a study by the World Economic Forum in 2020 [19], companies can significantly increase their resilience to cyberattacks by continuously improving their security measures.

2.1.3. Significance for companies

Implementing effective cyber risk management strategies is critical for organizations of all sizes and industries. Cybersecurity is no longer just a technical challenge but a business-critical factor that affects the entire organization. Companies that invest in cyber defenses and develop robust risk management strategies can ensure economic stability and gain a competitive advantage [13].

Figure 4 shows a 2023 study by Hiscox that shows that the risk of a cyberattack on companies is an increasing threat. The study records an increase in cyberattacks worldwide from 2021 to 2023.

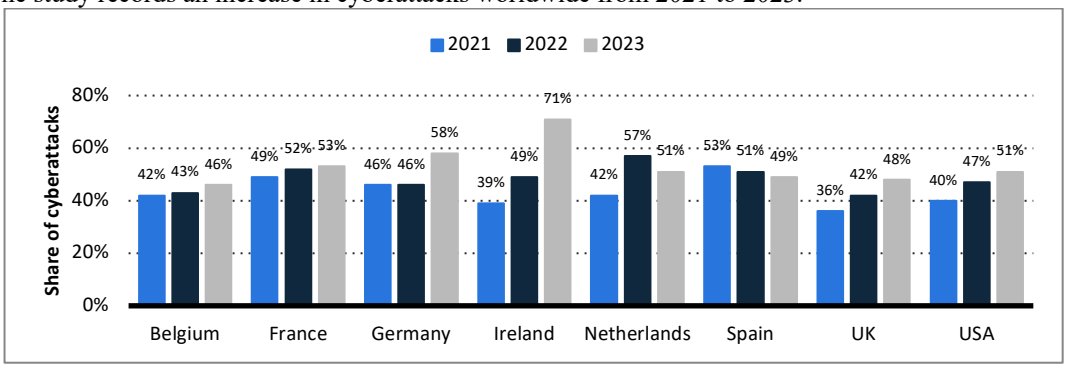

Fig. 4. Share of companies that experienced cyberattacks by country 2021-2023. Source: Hiscox

Overall, the literature shows that comprehensive and well-integrated cyber risk management is essential to counteracting cyberattacks' economic impact. Companies must proactively protect their digital infrastructures and strengthen their economic resilience.

2.2. Methodology

2.2.1. Literature research and case study

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].

2.2.2. Summary of the methodology

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.

2.3. Results

2.3.1. Economic Effects of Cyber Attacks

The empirical analysis reveals significant economic repercussions for companies that are victims of cyber-attacks. The primary economic impacts identified include direct financial losses, operational disruptions, and long-term reputational damage.

Direct Financial Losses: The immediate costs associated with cyber-attacks are substantial. These costs encompass IT repairs, legal fees, regulatory fines, and incident response expenses. For instance, data breaches can result in average costs of $4.24 million per incident [9]. Based on recent industry reporting, ransomware attacks have been found to incur costs averaging $1.85 million per incident, including ransom payments and system restoration expenses [17].

Operational Disruptions: Cyber-attacks often lead to significant operational disruptions, affecting business continuity. The study found that companies experienced an average downtime of 22 days post-attack, directly impacting productivity and revenue generation [6]. Furthermore, supply chain disruptions were noted, particularly in sectors heavily reliant on digital operations, such as manufacturing and logistics [1].

Reputational Damage: Long-term reputational damage following a cyber-attack can lead to customer trust and market share loss. Companies reported an average 10% decline in customer base within the first year after the attack, highlighting the critical need for effective crisis communication and reputation management strategies [15].

2.3.2. Effectiveness of Cyber Risk Management Strategies

The analysis also evaluated the effectiveness of various cyber risk management strategies companies employ to mitigate the impacts of cyber-attacks. The key findings are as follows:

Proactive Cybersecurity Measures: Companies that invested in proactive cybersecurity measures, such as regular security audits, employee training, and advanced threat detection systems, reported a 50% reduction in the frequency of successful attacks [13]. These measures are critical in identifying and mitigating potential threats before they cause significant harm.

Incident Response Planning: Effective incident response planning significantly reduced recovery time and costs. Companies with robust incident response plans, including defined roles and responsibilities and regular simulation exercises, experienced a 35% faster recovery time and 25% lower financial losses than those without such plans [14].

Cyber Insurance: Adopting cyber insurance provided financial protection and facilitated quicker recovery from cyber incidents. Companies with cyber insurance coverage reported 40% lower out-of-pocket expenses and benefited from access to specialized incident response services provided by insurers.

Integration of Cyber Risk into Corporate Governance: Firms that integrated cyber risk management into their corporate governance structures demonstrated improved resilience. This integration involved regular reporting to the board, aligning cybersecurity strategies with business objectives, and fostering a culture of security awareness. These companies experienced a 30% reduction in both the frequency and severity of cyber incidents [19].

2.4. Summary of Key Findings and Implications for Practice

The empirical analysis highlights the profound economic impacts of cyber-attacks on companies and underscores the importance of effective cyber risk management strategies. The key findings can be summarized as follows:

Cyber-attacks lead to substantial direct financial losses, operational disruptions, and long-term reputational damage. Proactive cybersecurity measures, effective incident response planning, cyber insurance, and integration of cyber risk into corporate governance are critical in mitigating the impacts of cyber-attacks. Companies that adopt a comprehensive approach to cybersecurity, combining technological solutions with organizational practices, demonstrate greater resilience to cyber threats.

2.5. Implications for Practice

The findings suggest several implications for practice.

Investment in Cybersecurity: Companies should allocate adequate resources towards cybersecurity measures, including technology investments and employee training, to reduce the likelihood of successful attacks.

Development of Incident Response Plans: Establishing and regularly updating incident response plans is essential for minimizing recovery time and costs.

Adoption of Cyber Insurance: Companies should consider cyber insurance as part of their risk management strategy to provide financial protection and access to expert incident response services.

Corporate Governance Integration: Integrating cyber risk management into corporate governance structures can enhance overall organizational resilience and ensure that cybersecurity is a priority at the highest levels of management.

3. Case Study: Detailed Analysis

Norsk Hydro ASA, a Norwegian aluminum manufacturer, was the victim of a major cyberattack by ransomware known as "LockerGoga" in March 2019. This attack led to significant operational disruptions and economic losses. Norsk Hydro is a global company with around 35,000 employees and production facilities in 40 countries, significantly increasing the attack's scope [8].

3.1. Detailed description of the incident

On March 19, 2019, Norsk Hydro's IT systems were infected by the LockerGoga ransomware. The attackers accessed the company's networks and began encrypting files, taking down numerous systems and production facilities. The production facilities in Europe and the USA and the company's administrative and communication systems were affected.

3.2. Economic Impact

Direct effects:

- Production losses: The attack led to production losses at several plants, especially in Norway and Germany. The total loss due to production interruptions was estimated to be around USD 40 million to USD 50 million [8]
- IT recovery costs: Restoring IT systems and purchasing new hardware and software licenses cost millions.

Indirect effects:

- Loss of trust: The attack damaged the confidence of customers and investors. Norsk Hydro's share price fell immediately after the attack became known.
- Reputational damage: Media coverage of the incident resulted in significant reputational damage, which had a long-term impact on the company's image.
- Long-term investments: Norsk Hydro significantly improved its IT security infrastructure and trained its employees to prevent future attacks.

3.3. Measures and actions taken

Norsk Hydro responded to the attack by taking affected systems offline and continuing production manually where possible. It worked closely with cybersecurity experts and government agencies to analyze the attack and restore the systems. In addition, it refused to pay the demanded ransom and instead relied on its own resources to restore the data.

3.4. The long-term strategy

Following the attack, Norsk Hydro implemented comprehensive measures to improve their cybersecurity strategies, including:

- Implementation of advanced security technologies such as enhanced firewalls and intrusion detection systems.
- Regular security audits and penetration tests to identify and remediate vulnerabilities.
- Intensive training programs for employees to raise awareness and prevent cyber threats.

3.5. Summary of the case study

Norsk Hydro ASA's case study impressively illustrates a cyber attack's far-reaching economic and organizational impact and the need for robust cyber risk management strategies. This case study provides valuable insights for other companies looking to arm themselves against similar threats through the detailed analysis of the incident and the responses and actions described.

3.6. Conclusion

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/