Replication Study: Defining Cyber Risk

Nawaris Almerza,[1a], Dawn Childs[1b], and Justin Hogg[1c]

[1] Marymount University, Arlington VA 22207, USA
[a]nawaris_almerza@marymount.edu, [b]dawn_childs@marymount.edu,
[c]justin_hogg@marymount.edu

Abstract. As the world continues to undergo a rapid digital transformation, the size of exposed attack surfaces correspondingly increases the level of cyber risk across the industry, the significance of that risk, and the requirement for a shared understanding of what constitutes a cyber risk. To properly study and understand this increase in cyber risk commonly agreed-upon definition for the term is essential. And yet, a lack of documentation exists regarding the term's meaning, and no definitive description persists across the industry. In 2020, Grzegorz Strupczewski attempted to address this shortfall in Defining Cyber Risk. In that publication, Strupczewski presented a comparative content analysis of the term covering nearly 20 years of peer-reviewed works, resulting in a proposed definition that addresses the dimensions he identified during his research. This research study replicates the methodology employed by Strupczewski on more recent scholarly articles, seeking to determine whether Strupczewski's proposed definition was still comprehensive or whether changes in usage of cyber risk in cybersecurity publications suggest that an amended description of the term is appropriate.

Keywords: Replication Study, Cyber Risk, Cybersecurity.

1 Introduction

Organizations worldwide continue to implement digital transformation strategies, resulting in an increase of vulnerable cyber landscapes and the likelihood that significant cyber incidents negatively affect society. The constancy of this rate of digital change places considerable importance on understanding and mitigating risks to cyberinfrastructure. This change also implies the importance of establishing and adhering to a shared agreement in defining what cyber risk constitutes at a fundamental level.

In 2020, Polish researcher Grzegorz Strupczewski published the results of his comparative content analysis study that researched scholarly publications to extract and present a standard definition for the concept of cyber risk [1]. This work was academically interesting, conveying the efforts to process hundreds of research articles published between 2000 and 2018 to extract applicable definitions from those works, analyze and code their descriptions, culminating in a comprehensive proposal definition that combined all aspects of previous results while remaining unique [1].

Given increasing attention and developments in the cybersecurity industry, the proposition of replicating Strupczewski's original work intrigued this research team. According to Peels, a replication study may apply the same research protocol to the same data set as an initial study, use the same research protocol to a new data set, or incorporate a new data set and a revised research methodology [2]. This research team concluded that applying the same methods to a more recent data set might provide potential insights beyond a direct repeat of Strupczewski's initial effort. As such, the purpose of this replication study is to extend Strupczewski's initial article to incorporate more current reporting to determine whether his initial analysis and conclusions are still sound or whether they may require further considerations and adjustments over time. Another aim of this study is to evaluate whether Strupczewski's proposed definition was still sufficiently comprehensive.

2 Methodology/Limitations

The goal of this research team was to replicate Strupczewski's methodology as closely as possible, incorporating newer articles that may result in changes to terms and definitions, which may show a change over time that strays from Strupczewski's initial work. However, this research team acknowledges the time and resource limitations that may affect the replication study results. Of note, Strupczewski utilized several journal databases, including EBSCOhost, Google Scholar, the Social Science Research Network (SSRN), and Science Direct, all available to the research team [1]. However, the team acknowledges several limitations that may affect this replication study's results. First, the renaming of several database collections used in Strupczewski's initial study may result in different databases used in the replication. Additionally, this research team utilized database licenses procured through Marymount University, which were not comprehensive for all databases and may have limited the potential data set analyzed in the replication content analysis.

It is worth noting that should this research team discover articles containing definitions of cyber risk that correspond to sources previously established by Strupczewski, they will be indicated as still in use and confirm that the initial data is still relevant. Equally as important, this team will seek to find new and previously undocumented definitions of cyber risk in the more recent literature to establish whether Strupczewski's previously identified components and proposed overarching characterization for cyber risk are still valid.

3 Results of Replication

In his research efforts, Strupczewski identified over 200 articles created between 2000 and 2018 in his data pool, from which he extracted 20 definitions of cyber risk, the categorization of which explored whether they contained one or more of three components: a source of cyber risk, risk objects, and impacts of cyber risk [1]. In subsequent searching of articles between January 2019 and November 2021, this research team

compiled an exhaustive list of 474 peer-reviewed journal articles by duplicating Strupczewski's methodology.

In reviewing the available literature at the time of publication, Strupczewski identified 20 definitions of cyber risk in peer-reviewed journals published between 2000 and 2018 [1]. Conversely, this research team identified a total of 20 distinct definitions of cyber risk in articles published between 2019 and 2021, of which seven definitions Strupczewski also cataloged in his initial research. Table 1 outlines those definitions below.

Table 1. Definitions of Cyber Risk.

Source of Definition	Definition
Abdullah, Ali, Malebary, Ahmed [3]	"Cyber risk is the potential loss or damage that might impact the system by a threat advanced from the system vulnerabilities."
Aneja, Manocha, Verma, Kathuria [4]	"Cyber risk signifies any risk of money-related misfortune, interruption, or harm to the notoriety of an association from a disappointment of its information technology frameworks."
Bank for International Settlements [5][1]	"The combination of the probability of an event occurring within the realm of an organisation's information assets, computer and communication resources and the consequences of that event for an organisation."
Bank for International Settlements [6]	"Cyber risk commonly refers to the risk of financial loss, disruption, or reputational damage to an organisation resulting from the failure of its IT systems. These episodes include malicious cyber incidents (cyber attacks) where the threat actor intends to do harm (e.g., ransomware attacks, hacking incidents or data theft by employees)."
Biener, Eling, Wirfs [7]	"Cyber risk may be defined as a function of 3 parameters: (i) Impact expresses the level of damage that a given risk may cause; (ii) Threat expresses whether or not a given risk is probable; Vulnerability expresses whether or not existing (iii) information security measures are effective."
Brewer [8] [2]	"Cyber risk is a vulnerability (i.e., weakness) that may be exploited by threats to gain access to certain assets. It is measured by multiplying threat, vulnerability and asset value."
Carter, Mainelli [9]	"Cyber risk, the risk to people and businesses posed by information & computing technology (ICT), is multi-faceted,

[1] Denotes a definition used in articles found by Strupczewski and this research team.
[2] Denotes a definition used in articles found by Strupczewski and this research team.

	potentially leading to loss of data, revenues, direct physical harm, or reputation."
Cebula, Young [10]	"Cyber risk is defined as operational risks to information and technology assets that have consequences affecting the confidentiality, availability or integrity of information or information systems."
Cheung, Bell [11]	"Cyber risk resides in cyberspace, so its elimination or reduction belongs to the field of risk management."
Eling, Schnell [12] [3]	"Cyber risk encompasses any risk emerging from the use of information and communication technology (ICT) that compromises the confidentiality, availability, or integrity of data or impairment services. The impairment of operational technology (OT) eventually leads to business disruption, (critical) infrastructure breakdown, and physical damage to humans and properties. Cyber risk is either caused by natural disasters or is man-made where the latter may emerge from human failure, cyber criminality (e.g. extortion, fraud), cyberwar or cyber terrorism. It is characterised by interdependencies, potential extreme events, high uncertainty with respect to data and modeling approach, and the risk of change."
Financial Stability Board [13]	"The combination of the probability of cyber incidents occurring and their impact. Source: Adapted from CPMI-IOSCO, ISACA Fundamentals (definition of 'Risk') and ISACA Full Glossary (definition of "Risk")."
Institute of Risk Management [14] [4]	"Cyber risk means any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems."
Jevtić, Lanchier [15]	"Cyber risk due to breach is 'the risk of a financial loss caused by a breach of an institution's IT infrastructure by unauthorized parties, resulting in exploitation, taking possession of, or disclosure of data assets.'"
Kavallieratos, Spathoulas, Katsikas, Zeadally [16]	"Cyber risk is evaluated as a function of the likelihood of an adverse event, such as an attack, occurring; and of the impact that will result when the event occurs."

[3] Denotes a definition used in articles found by Strupczewski and this research team.
[4] Denotes a definition used in articles found by Strupczewski and this research team.

Lu, Huang, Azimi, Guo, [17]	"Cyber risk refers to bad behavior such as fraud due to insufficient security or design flaws."
Nifakos et al. [18]	"Exposure to harm or loss resulting from breaches of or attacks on information systems."
National Institute of Standards and Technology [19]	"A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence."
Nguyen-Phuoc, Oviedo-Trespalacios, Vo, Le, Nguyen [20]	"Cyber risk relates to the risks presented by an online environment, such as data security."
Pei, Jin, Yang [21]	"The term 'cyber risk' usually refers to cybersecurity incidents that lead to losses to a firm."
Refsdal et al. [22] [5]	"Cyber risk is a risk that is caused by a cyber-threat occurring in cyberspace."

Strupczewski categorized the 20 definitions he found against three dimensions of cyber risk: the sources of cyber risk, the risk objects, and the impact of cyber risk [1]. The sources of cyber risk constitute vulnerabilities or weaknesses in an organization's digital or physical infrastructure, which might be exploited [8]. The concept of risk objects encapsulates hardware, software, or other elements from which cyber risk may originate [1]. The third category, the impact of cyber risk, considers the adverse effects of a cyber risk regardless of whether the threats posed are malicious or accidental [1]. Similar to the categorization performed in Strupczewski's initial publication, Table 2 displays this research team's analysis results below.

Table 2. Key Components in the Cyber Risk Definitions.

Source of Definition	Name of Key Component			Number of Key Components per Definition
	Source of Cyber Risk	Risk Objects	Impact of Cyber Risk	
Abdullah, Ali, Malebary, Ahmed [3]		■	■	2
Aneja, Manocha, Verma, Kathuria [4]		■	■	2
Bank for International Settlements [5] [6]		■		1

[5] Denotes a definition used in articles found by Strupczewski and this research team.
[6] Denotes a definition used in articles found by Strupczewski and this research team.

Bank for International Settlements [6]	■	■	■	3
Biener, Eling, Wirfs [7]		■		1
Brewer [8] [7]	■			1
Carter, Mainelli [9]	■	■	■	3
Cebula, Young [10]		■	■	2
Cheung, Bell [11]		■		1
Eling, Schnell [12] [8]	■	■	■	3
Financial Stability Board [13]		■		1
Institute of Risk Management [14] [9]	■		■	2
Jevtić, Lanchier [15]	■	■	■	3
Kavallieratos, Spathoulas, Katsikas, Zeadally [16]	■		■	2
Lu, Huang, Azimi, Guo, [17]	■	■	■	3
Nifakos, et al. [18]	■	■	■	3
National Institute of Standards and Technology [19]	■	■	■	3
Nguyen-Phuoc, Oviedo-Trespalacios, Vo, Le, Nguyen [20]		■		1
Pei, Jin, Yang [21]	■		■	2
Refsdal, Solhaug, Stølen [22] [10]	■			1

In his initial publication, Strupczewski identified one peer-reviewed article containing a definition of cyber risk, which addressed all three categories: risk source, risk object, and risk impact, published in 2016 by Eling and Schnell [1]. As noted in Table 2 above, the results of this replication included references to that definition and the identification

[7] Denotes a definition used in articles found by Strupczewski and this research team.
[8] Denotes a definition used in articles found by Strupczewski and this research team.
[9] Denotes a definition used in articles found by Strupczewski and this research team.
[10] Denotes a definition used in articles found by Strupczewski and this research team.

of six additional definitions that incorporated all three components of cyber risk. Those six other definitions do not incorporate search results that included Strupczewski's paper, which forms the basis of this replication study. Additionally, this replication study did not identify any definitions of cyber risk, which introduced new dimensions or facets that exceeded the proposed comprehensive definition proposal made by Strupczewski [1].

4 Implications of the Replication Study

During this replication study, this research team focused on a publication period of 2019 through 2021, resulting in a data set of 474 articles, more than twice the number of scholarly analyzed in Strupczewski's initial content analysis, which examined works published between 2000 and 2018 [1]. This increase in publications suggests a possible heightened focus upon the concept of cyber risk in a world that is increasingly dependent upon security digital technologies in cyberspace. Additionally, while Strupczewski found only one article defining cyber risk using all three categorical dimensions, this research team discovered a total of seven definitions using all three categorial dimensions during the replication study [1]. The increase in comprehensive descriptions implies a potentially growing awareness of the multiple facets of cyber risk.

It is worth noting that of 474 articles reviewed in this replication study, there were only 20 unique included definitions of cyber risk. This significant minority constitutes fewer definitions by percentage than observed in Strupczewski's initial work [1]. As previously noted, limitations in access to some results in the journal databases due to paywalls and membership may have affected these results.

Further research could extend the results of this replication study by seeking to observe whether the definition for cyber risk proposed by Strupczewski is still comprehensive at that time. Other additional research could explore reasons for the relative percentage decrease in publications that provide definitions for cyber risk while still incorporating the term as an aspect in their work.

5 Conclusion

The results of this replication confirm growing scholarly attention on core concepts of cyber risk over time. A replication study of the methods employed by Strupczewski using a more recent data set supports his initial comparative analysis. This new research suggests that the initial dimensions of cyber risk and the proposed comprehensive definition made by Strupczewski remain consistent with the descriptions of cyber risk used by subsequent academic scholars over the last three years.

References

1. Strupczewski, G.: Defining cyber risk. Safety Science 135(105143) 1-10 (2021)
2. Peels, R.: Replicability and replication in the humanities. Research Integrity and Peer Review 4(1), 1-12 (2019)

3. Abdullah, T., Ali, W., Malebary, S., Ahmed, A.: A Review of Cyber Security Challenges, Attacks and Solutions for Internet of Things Based Smart Home. International Journal of Computer Science and Network Security 19(9), 139-146 (2019)
4. Aneja, P., Manocha, M., Verma, S., Kathuria, M.: An overview of cyber risks in Internet of Things (IoT) world. International Journal for Research in Applied Science and Engineering Technology 8(6) 268–272 (2020)
5. Bank for International Settlements, https://www.bis.org/cpmi/publ/d146.htm. Last accessed 7 Feb 2022
6. Bank for International Settlements, https://www.bis.org/publ/work865.htm. Last accessed 7 Feb 2022
7. Biener, C., Eling, M., Wirfs, J.: Insurability of cyber risk: An empirical analysis. The Geneva Papers on Risk and Insurance - Issues and Practice 40(1) 131–158 (2015)
8. Brewer, D.: Risk assessment models and evolving approaches. IAAC SENATE HOUSE WORKSHOP. London, UK (2000)
9. Carter, S., Mainelli, M.: Cyber-catastrophe insurance-linked securities on smart ledgers (SSRN scholarly paper ID 3675420). Social Science Research Network 1-75 (2018)
10. Cebula, J. Young, L.: A taxonomy of operational cyber security risks The Software Engineering Institute, 1-47 (2010)
11. Cheung, K., Bell, M.: Attacker–defender model against quantal response adversaries for cyber security in logistics management: An introductory study. European Journal of Operational Research, 29(2), 471-481 (2019)
12. Eling, M., Schnell, W. What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance, 17(5), 474–491 (2016)
13. Financial Stability Board, https://www.fsb.org/wp-content/uploads/P121118-1.pdf. Last accessed 7 Feb 2022
14. Institute of Risk Management, https://www.theirm.org/what-we-say/thought-leadership/cyber-risk. Last accessed 7 Feb 2022
15. Jevtić, P., Lanchier, N.: Dynamic structural percolation model of loss distribution for cyber risk of small and medium-sized enterprises for tree-based LAN topology. Insurance: Mathematics and Economics, 91, 209–223 (2020)
16. Kavallieratos, G., Spathoulas, G., Katsikas, S., Zeadally, S.: Cyber risk propagation and optimal selection of cybersecurity controls for complex cyberphysical systems. Sensors (14248220), 21(5), 1691 (2021)
17. Lu, H., Huang, K., Azimi, M., Guo, L.: Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks. IEEE Access, 7, 41426–41444 (2019)
18. Nifakos, S., Chandramouli, K., Nikolaou, C., Papachristou, P., Koch, S., Panaousis, E., Bonacina, S.: Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors (14248220), 21(15), 5119 (2021)
19. National Institute of Standards and Technology. Security and privacy controls for federal information systems and organizations, special publication 800-53 revision 5 (2013)
20. Nguyen-Phuoc, D., Oviedo-Trespalacios, O., Vo, N., Le, P., Nguyen, T.: How does perceived risk affect passenger satisfaction and loyalty towards ride-sourcing services? Transportation Research Part D: Transport and Environment, 97, 102921 (2021)
21. Pei, R., Jin, Z., Yang, Z.: Cyber-attacks measurement for public companies: An empirical analysis (SSRN scholarly paper ID 3607614). Social Science Research Network, 1-12, (2020)
22. Refsdal, A., Solhaug, B., Stølen, K.: Cyber-risk management. Springer International Publishing, Cham, Switzerland (2015)