Improving the Cybersecurity Awareness of Finnish Podiatry SMEs

JYRI RAJAMÄKI, NIROJ CHAULAGAIN, MARKUS KUKKONEN, PESSI NURMI, MIKKO HONKONEN, SAMU SAARINEN, TORSTI KINNUNEN
Unit W,
Laurea University of Applied Sciences,
Vanha maantie 9, 02650 Espoo,
FINLAND

Abstract: - In the health and welfare sector, many entrepreneurs and employees are not skilled in information and cybersecurity, even when they are constantly dealing with sensitive data. This case study research examines a team of private Finnish podiatrists and their cybersecurity capabilities. The goal of the study is to gather the most important information and cybersecurity topics and create an easy-to-read guide that helps businesses find the framework for their information and cybersecurity and address it in more detail. The results of the case study show that the target organization's most important information and cybersecurity areas are phishing, secure environment, secure communication, passwords, software updates, backups, and physical security. Understanding these topics and following the planned guidelines will strengthen the security posture of all small and medium-sized enterprises (SMEs) in the health and welfare sector.

Key-Words: - Cyber-attack, cybercrime, cybersecurity, cyber threats, health, healthcare, phishing, ransomware

Received: June 29, 2022. Revised: August 17, 2023. Accepted: September 20, 2023. Published: October 25, 2023.

1 Introduction

The project 'Dynamic Resilience Assessment Method including combined Business Continuity Management and Cyber Threat Intelligence Solution for Critical Sectors' (DYNAMO) develops a platform that enables the resilience assessment of critical sectors (health, energy, and transportation) by combining the disciplines of Business Continuity Management (BCM) and Cyber Threat Intelligence (CTI). Cybersecurity can be thought of as a secure barrier around an organization's most asset. When well organized and widely applied, cybersecurity measures can improve business continuity. Figure 1 shows how cybersecurity can be seen as a circle around business continuity. Comprehensive cybersecurity is based on appropriate cyber skill levels and well-functioning, reliable technical environments. None of these guarantees security, they are needed together, and technical environments must be configured and used ethically to ensure privacy when using business information technology (IT) applications, [1]. This case study addresses the impact of cyber awareness on business continuity for small healthcare and welfare businesses; the case is Finnish podiatrists.

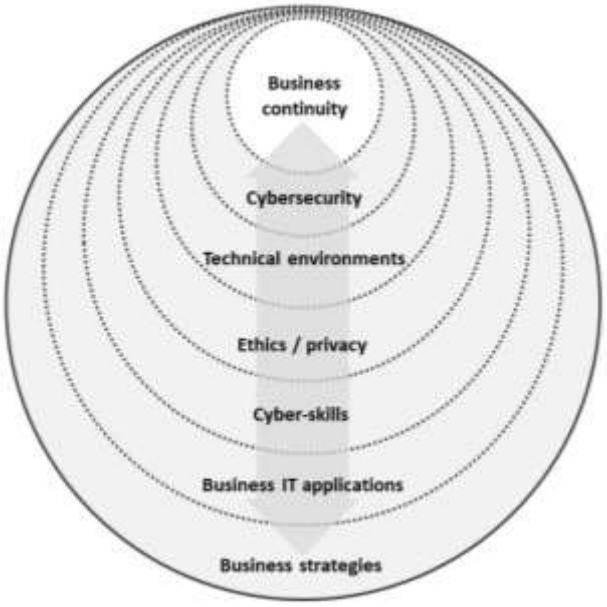

Fig.1: Model of the dimensions of business continuity and cybersecurity (modified from, [1])

The use of digital technologies and electronic health records in the health and welfare industry has skyrocketed, [2]. On the other hand, current challenges in cybersecurity are the biggest obstacle to the expansion of such digital services, [3]. Recently, several data breaches have occurred

through malware, insiders, lost devices, and accidental disclosure highlighting the importance of cybersecurity, [4]. Cybersecurity can have a serious impact on small businesses. ENISA surveyed small and medium-sized enterprises (SMEs) and 90% said a cyber-attack would have a serious negative impact, and 57% said they would likely go bankrupt, [5]. SMEs unfortunately have budget constraints and limited IT resources. However, good cyber hygiene can significantly improve cybersecurity at almost no additional cost through employee awareness, [6]. Ethical and resilient electronic health and well-being systems include analyses of attack vectors, threats, vulnerabilities, and risks to specify a comprehensive cybersecurity architecture for electronic health and well-being systems, [7].

Phishing attacks have become an increasingly prevalent threat to organizations of all kinds, including those in the healthcare and welfare industry, [8]. These attacks involve the use of fraudulent emails, text messages, or other forms of digital communication to trick individuals into divulging sensitive information such as login credentials or financial details. In the health and welfare sector, where the security of patient data is of paramount importance, phishing attacks can have devastating consequences. Not only can they result in the theft of confidential medical records, but they can also compromise the safety and well-being of patients.

The main objective of this case study research is to raise cybersecurity awareness in an SME concerning the common topics related to cybersecurity in the health and welfare sector. The research findings provide a comprehensive foundation for improving cybersecurity practices and offer guidance to SMEs that face unique challenges in protecting sensitive data and ensuring business continuity. Ultimately, we hope that this paper will serve as a valuable resource for healthcare and welfare professionals and IT administrators seeking to safeguard their organizations against the growing cyber threats. The paper is structured in four sections: Section 1 is an introduction to the study, Section 2 describes the research methodology and design, Section 3 presents the results, and Section 4 summarizes the study and presents the conclusions.

2 Research Methodology and Design

The research approach of this study is a case study, which is suitable as a research approach when the goal is to deeply understand the development target and produce development proposals. Case studies can be used to understand, for example, the mutual relations and activities of employees in organizations with customers. Often there is only one subject to be investigated and the research is often focused on, for example, a function or a process. Qualitative case study methodology provides the researcher with tools to study multiple phenomena in their context, [9].

A case study analysis relies on multiple sources of evidence with data needing to converge in a triangulation fashion, and it benefits from the prior development of theoretical propositions to guide data collection and analysis, [10]. ‘Triangulation’ refers to the use of multiple sources of evidence, such as data sources and different researchers, in the same study, [11], [12].

The goal of the research is to determine how information and cybersecurity for entrepreneurs within the target organization, Jalkapaiva, can be enhanced. The Jalkapäivä team comprises private podiatrists from various regions of Finland. The research primarily aims to comprehend the current state of the organization and the ways different functions influence the development of information and cybersecurity. Since this specific phenomenon has not been previously examined within the organization, a case study is considered an ideal approach.

At the onset of the research, the researchers familiarized themselves with the target organization, the health and welfare sector, and the subject of the research, which is information and cybersecurity and how it takes shape. Yin's case study methodology, [10], served as the framework for the research process, described as an iterative operational model. The study's design and implementation are illustrated in Figure 2.

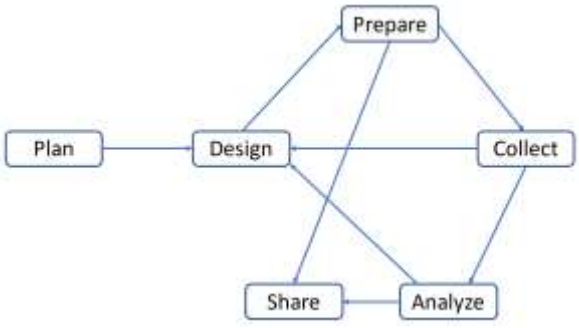

Fig. 2: Phases of Case Study Research, [10]

The research question addressed in the analysis stages is "How cyber vulnerability or weakness can be understood in the target organization and what means exist to reduce that vulnerability." The unit of

analysis is collectively discussed and considered as a deficiency, vulnerability, or weakness. The paper provides the results of the case study analysis by identifying weaknesses called vulnerabilities and improvement measures to integrate cybersecurity called mitigation actions.

Triangulation is used in the analysis in the following form: 1) data sources as data triangulation (multiple literature references, several interviews in the target organization, and familiarization with the target organization's documents); and 2) among different researchers as investigator triangulation. The process included qualitative data from the literature, interviews, and the target organization's documents which are analyzed in terms of systematic categorization as data reduction, displays, and drawings of data, [12], [13]. The used form of analysis refers to data reduction as the process of selecting, focusing, simplifying, and abstracting the used research data collection.

3 Research Findings

This chapter provides the results of the case study analysis by identifying weaknesses as well as remedial measures to improve cybersecurity at the target organization.

3.1 Phishing Attacks

3.1.1 Phishing Vulnerability

Phishing attacks are the most common ransomware attacks in the health and welfare sector because they target the most vulnerable link in the security chain. Users often lack sufficient knowledge or resources to fight against the attacks. Several studies show that lack of time is a big reason for healthcare personnel falling victim to phishing attacks, [14], [15]. The lack of time is a larger factor in attacks than the lack of technical knowledge or lack of interest to avoid the attacks. According to, [16], a strong correlation exists between heavy workload and susceptibility to phishing attacks, [16]. Similar results have been reported on case studies and simulations, strongly suggesting that a great way to prevent phishing attacks in healthcare and welfare is to provide the personnel time to go through the emails, [17], [18].

In addition to lack of time, additional factors for successful phishing attacks are the use of technology and appeal to authority or urgency, [19]. On the other hand, smartphones cause more phishing emails to succeed than desktop computers. This is because phone applications tend to hide the URL addresses from the messages, while desktop applications display them, [17].

The goal of the attackers often seems to be credentials to different systems. For example, The Office of the Data Protection Ombudsman, which is a government official under the Finnish Ministry of Justice states that the majority of reported phishing attempts involve Office 365 credentials.

According to a white paper by F-secure, IT workers click on phishing emails as often as other employees, suggesting that better IT skills and additional cybersecurity training may not necessarily help achieve the desired goal. The same study found that ease of reporting increases the rate at which suspicious emails are reported. Furthermore, the study again found support for the claim that giving enough time to study the content of an email improves the ability to recognize malicious emails. When employees feel trusted, they have greater intentions to comply with security policies. However, the compliance intention did not significantly correlate with compliance behavior, [14].

3.1.2 Risk Mitigation

Based on the analysis of the case study, the following conclusions and suggestions were made on how to reduce the risk of clicking on a phishing link in the target organization. The entrepreneurs belonging to the target organization want to follow the rules and guidelines, but despite the best intentions, people click on harmful links. Educating personnel on cybersecurity is crucial, but knowing the dangers does not always prevent clicking on links, and the threat may not seem imminent.

Additional understanding of attack vectors would demand significant training in non-healthcare-related topics. Studies have shown that even IT department employees are susceptible to clicking on these links. This indicates that additional technical know-how is not a feasible solution. It does not guarantee immunity to attacks and would require extensive training for employees.

Multiple sources mention the hectic environment in the healthcare and welfare industry as a contributing factor. Employees are often pressed for time, leading to hasty decisions. The key to improving cybersecurity in such an environment is to drastically reduce the number of emails an entrepreneur or employee receives during the workday. Creating a work culture where unnecessary messaging via email is minimized can help. This involves sending fewer emails and only to those directly concerned. The reduction of unnecessary email traffic should occur by moving as

much internal messaging as possible to collaboration platforms like Slack or Teams and the organization's intranet. By reducing email fatigue and giving more attention to remaining messages, the likelihood of falling for phishing emails decreases. This approach should improve the work environment and help combat phishing emails in the healthcare industry.

3.2 Safe Environment

3.2.1 Privacy Filters

When operating in public spaces, privacy filters can reduce data leakage. According to ViewSonic, 91% of visual hacks are successful, with 52% of the leaked sensitive data occurring through the display screen. Privacy filters are one of the best security-enhancing products, [20].

To prevent data leaks, entrepreneurs and their employees should use privacy filters on their endpoint screens when working in public spaces or customer premises.

3.2.2 Open Wi-Fi Networks

Using an open Wi-Fi network is a security risk that exposes your computer's network connection. The network connection is not encrypted between the Wi-Fi access point and your computer, allowing a malicious actor to capture your data packet for further use, [21].

Open Wi-Fi networks are a significant security risk, and it is not recommended to use them without a separate virtual private network (VPN) service due to the potential risk of tracking and data leaks.

3.2.3 VPN Connections

A VPN creates an encrypted connection between devices. Since a VPN connection creates an encrypted tunnel between devices, data transfer can be secured even in the most insecure network connections. When choosing a VPN service provider, it is essential to consider their reliability and the laws of the country where the company is operating.

3.2.4 USB Attacks

Universal serial bus (USB) devices are not always safe and can be used for attacks, so it is crucial to use physical barriers or software solutions such as disabling USB ports and ensuring employees understand the risks, [22].

3.3 Secure Communication

Communication security is a crucial part of any business, regardless of its size. We need to be able to communicate with our customers and each other. When it comes to the safety and security of communication, we must remember that sensitive data is regulated by multiple legislations, including, but not limited to, the General Data Protection Regulation (GDPR) and the Data Protection Act. These regulations originate from both the EU and national levels and are divided into sets of laws and regulations. All processing of customer data should adhere to these laws and regulations. There are many ways to enhance communication security, and the key is to remember what you are communicating, and which channel you are using. Secure instant messenger apps like Signal or Threema can be utilized. Emails can be secured using popular email applications like Outlook or Gmail, or one can choose to use secure email services like ProtonMail. Social media is an excellent way to contact and communicate with potential customers, but it is important to consider these platforms inherently insecure. A good practice is to use separate email accounts for different purposes.

3.4 The Importance of the Password

Good passwords must meet certain characteristics: complexity, length, unpredictability, uniqueness, and regular changes. Additionally, a good password should be easy to remember. Passwords represent the simplest and most cost-effective means of bolstering cybersecurity. They serve as crucial barriers against unauthorized access, thwarting malicious actors from infiltrating personal and organizational accounts. Countless examples of data breaches exist, in which malicious actors gained initial access through weak passwords.

The easiest way to ensure that passwords meet requirements is by utilizing password managers. These tools are invaluable for individuals and organizations in maintaining strong and secure passwords. Several password manager software options are available, ranging from free to subscription-based, and can be used on mobile devices, tablets, or computers. Examples include LastPass, 1Password, and Dashlane, as well as device-specific software like Apple's Keychain.

3.5 Software Updates

In the ever-changing world of cybersecurity, up-to-date systems are a crucial part of any cybersecurity plan. Cybercriminals evolve new tools and attack vectors every day, making it essential to ensure that your system is not vulnerable by keeping it updated to the newest version. Software updates are critical for maintaining the security and integrity of

software systems. They address vulnerabilities and weaknesses, fortifying the software against potential exploits and malicious attacks. Updates also incorporate enhanced security features and protocols, aligning the software with industry standards and mitigating emerging threats.

The best way to ensure that the software is updated is to have an updated policy. At its simplest, this involves conducting an update check at the end of the day. However, depending on the size and complexity of the system, a more comprehensive plan may be needed. For small and medium-sized businesses, implementing a robust update policy is one of the most important steps to improve cybersecurity resilience. Embracing a proactive approach towards software updates enables effective countermeasures against dynamic cyber threats. Stakeholders should prioritize and allocate resources for a stringent software update policy.

3.6 Backup of Critical Data

Backing up important files is crucial, and companies should make an inventory of critical data and categorize it while understanding laws governing data retention. When outsourcing backup to a cloud service provider, it is essential to consider the provider's service type, encryption details, encryption key/passphrase, data sharing process, and long-term data retention.

GDPR presents challenges for personal data storage in Europe, including the 'Right to be Forgotten'. Deleting personal data from backups is difficult and can leave data in older versions. Using unique identifiers (IDs) to replace personal data solves the problem and preserves backup files. Special care is needed for personal data databases and backups, [23].

3.7 Physical Security

The confidentiality, integrity, and availability of the resources can be protected when premises, people, information, and other physical assets are protected. Physical security along with physical security controls are equally important when considering cyber threats, [24].

Proper security controls in place can significantly improve the security posture of an organization. Preventive controls prevent unwanted events from happening in advance. Locks, mantraps, biometrics, keycards, etc. are preventive controls. Similarly, detective controls help in detecting unauthorized events. Motion detectors, door alarms, and fire/smoke alarms are detective controls.

Corrective controls correct a deviation from the standard state. Repairing a broken door, replacing a broken lock, fixing malfunctioning heating, ventilation, and air conditioning (HVAC) systems and humidity controls, etc. are corrective controls. Similarly, deterrent controls help in discouraging an attacker from attempting to breach a system or unauthorized access. Some examples include surveillance, guards on duty, warning signs, and more. On top of these, compensating controls can be utilized to compensate if a control is too costly or too complicated to maintain.

The organization should target layered physical security whenever possible starting from the perimeter security including fences, walls, and good lighting. Exterior security includes doors, windows, locks and keys, roofs, and common walls. Doors should have appropriate mechanisms and locks in place, windows with bars to stop force break-ins, and technology-oriented locks replacing traditional keys with magnetic keys.

Inner doors should also be always locked. Security badges can help avoid unauthorized people accessing the premises. Finally, the contents security needs to be considered, keeping critical hardware devices in a secured safe or vault, keeping the desk clean and hardware devices locked.

3.8 Clean Desk Policy and Secure Trash

The clean desk policy supports physical security. When an employee is not at the desk, confidential information should not be present on the desk such as documents containing customer information and flash drives containing sensitive information. Theft, loss, and unauthorized access to sensitive information can be prevented if these confidential documents and devices are stored out of sight in a vault. All employees must ensure that they do not leave the visitor alone in the office or near the computer system, [25].

Dumpster diving is a threat to an organization that deals with sensitive information. Hence, sensitive information containing personally identifiable information (PII), health records, financial data, and other confidential information should be disposed of safely and securely. Shredding, burning, pulping, degaussing, overwriting, and physical destruction can be done depending on whether the sensitive information is on the paper or devices.

3.9 Suggestions for Further Research

As a result of the research, the following ten suggestions for further research can be made:

1. Cybersecurity Training: Research the effectiveness of cybersecurity training in reducing susceptibility to phishing attacks among healthcare and welfare SMEs.
2. Employee Time Constraints: Investigate strategies to address time constraints among healthcare personnel and SME employees, reducing their vulnerability to phishing.
3. VPN Services: Compare different VPN service providers in terms of reliability and legal considerations for organizations in specific regions.
4. USB Device Security: Examine risks associated with USB devices and develop strategies for their secure use.
5. Secure Communication: Evaluate the effectiveness of secure communication tools and provide recommendations tailored to healthcare and welfare SMEs.
6. Password Security: Research the adoption and impact of password managers, focusing on usability and security.
7. Software Update Policies: Explore the development and implementation of software update policies for healthcare and welfare organizations.
8. Data Backup and GDPR: Investigate data backup practices and GDPR compliance in healthcare and welfare SMEs.
9. Physical Security Measures: Research the adoption and effectiveness of physical security measures, especially for organizations with limited resources.
10. Clean Desk Policies and Secure Trash Disposal: Evaluate the adoption and enforcement of clean desk policies and secure methods of sensitive information disposal in SMEs.

These research suggestions provide a comprehensive foundation for improving cybersecurity practices, particularly in the healthcare and welfare sector, and offer guidance for SMEs facing unique challenges in protecting sensitive data and ensuring business continuity.

4 Conclusions

Cybersecurity is an ever-evolving field. New threats emerge daily, and cybercriminals constantly find vulnerabilities in software and hardware. Small and medium-sized businesses are vulnerable to cyber-attacks, and a single ransomware incident can have devastating effects on a business, potentially leading to its demise. Only large corporations can afford highly sophisticated in-house security teams.

However, there are ways to combat and mitigate these threats. This study aims to identify mitigation tactics that are easy to implement and follow. Our primary goal is to provide valuable information that can be translated into actionable steps. Even small changes and investments can make a significant difference in a business's cybersecurity posture. To start, ensure that the devices are up to date with additional backups for business continuity in critical situations. The other things to consider are data compliance with rules and regulations, physical security, and the proper use of passwords with multi-factor authentication (MFA).

Our goal is to help business owners understand that despite the risks in cyberspace, there are simple and user-friendly ways to mitigate these threats. Implementing research-based recommendations can significantly improve a company's cybersecurity posture and at the same time improve business continuity. The remedies revealed in the study are not just for podiatrists, all SMEs can benefit from this study by following the guidelines.

Acknowledgement:
This work was supported by the DYNAMO project, which has received funding from the European Union's Horizon Europe research and innovation funding program under the grant agreement no. 101069601.

References:

[1] Frisk, I., Ruoslahti, H. & Tikanmäki, I., Cybersecurity through thesis in Laurea University of Applied Sciences, *Proceedings of the 22nd European Conference on Cyber Warfare and Security*, Vol. 22, No. 1, 2023, pp.484-492.

[2] Rajamäki, J., Towards Resilient Cyber-Physical eHealth Systems, *Proceedings of the 10th International Conference on Circuits, Systems, Signal and Telecommunications (CSST '16)*, WSEAS Press, 2016, pp.75-79.

[3] Rajamäki, J., SHAPES Cyber Secure HealthCare Platform in Digital Environments, *WSEAS Transactions on Communications*, Vol. 19, 2020, pp.18-25.

[4] Center for Internet Security (CIS), Data Breaches: In the Healthcare Sector, [Online] https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (Accessed Date: 12 March 2023).

[5] Kim, L., Cybersecurity awareness: Protecting data and patients. *Nursing*, Vol. 47, No. 6, 2022, pp.65-67.

[6] ViewSonic, Screen Privacy: How to protect yourself from visual hacking, January 17, 2021, [Online], https://www.viewsonic.com/library/tech/screen-privacy-how-to-protect-yourself-from-visual-hacking/ (Accessed Date: 6 March 2023).

[7] Rajamäki, J. & Hummelholm, A. Ethical Resilience Management Framework for Critical Healthcare Information Infrastructure, *WSEAS Transactions on Biology and Biomedicine*, Vol. 19, 2022, pp.67-76. https://doi.org/10.37394/23208.2022.19.9.

[8] Statista, Most commonly reported cyber crime categories in the United States in 2022, by number of individuals affected, https://www.statista.com/statistics/184083/commonly-reported-types-of-cyber-crime-global/ (Accessed Date: 6 May 2023).

[9] Baxter, P. & Jack, S., Quality case study methodology: Study design and implementation for novice researchers, *The Qualitative Report*, Vol. 13, No. 4, 2008, pp.544-559.

[10] Yin, R. K., *Case* study *research design and methods* (4th ed.), Sage Publications, 2009.

[11] Patton, M., *Qualitative evaluation and research methods* (2nd ed.), Sage Publications, 1990.

[12] Miles, M. B. & Huberman, A. M., *Qualitative data analysis: An expanded sourcebook*, Sage Publications, 1994.

[13] Robson, C., *Real world research* (2nd ed.), Blackwell Publishing, 2002.

[14] Jalali, M. S., Bruckes, M., Westmattelmann, D. & Schewe, G., Why Employees (Still) Click on Phishing Links: Investigation in Hospitals. *Journal of Medical Internet Research*, Vol. 22, No. 1, 2020, e16775.

[15] Rajamäki, J., Rathod, P., & Kioskli, K., Demand Analysis of the Cybersecurity Knowledge Areas and Skills for the Nurses: Preliminary Findings, *European Conference on Cyber Warfare and Security*, Vol. 22, No. 1, 2023, pp.711-716.

[16] Yeng, P. K., Fauzi, M.A., Yang, B. & Nimbe, P., Investigation into Phishing Risk Behaviour among Healthcare Staff, *Information*, Vol. 13, Issue 8, 2022, pp.392.

[17] Rizzoni, F., Magalini, S., Casaroli, A., Pasquale, M., Dixon, M., & Coventry, L., Phishing simulation exercise in a large hospital: A case study, *Digital Health*, Vol. 8, 2022, pp.1–13.

[18] Rozentals. E., *Email load and stress impact on susceptibility to phishing and scam emails*, Luleå University of Technology, 2021.

[19] Halevi. T., Memon. N. & Nov, O, Spear-phishing in the wild: a real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks, *SSRN eJournal*, January 2, 2015, [Online], https://ssrn.com/abstract=2544742 (Accessed Date: 5 May 2023).

[20] ViewSonic, Screen Privacy: How to protect yourself from visual hacking, Jan 17, 2021, [Online], https://www.viewsonic.com/library/tech/screen-privacy-how-to-protect-yourself-from-visual-hacking/ (Accessed Date: 22 September 2023).

[21] Sobh, T. S., Networks security and accessing control, *International Journal of Computer Network and Information Security*, Vol. 5, Issue 7, 2013, pp.9-20.

[22] Nissim, N., Yahalom, R. & Elovici, Y., USB-based attacks, *Computers & Security*, Vol. 70, 2017, pp.675-688.

[23] Politou, E., Michota, A., Alepis, E., Pocs, M. & Patsakis, C., Backups and the right to be forgotten in the GDPR: An uneasy relationship, *Computer Law & Security Review*, Vol. 34, Iss. 6, 2018, pp.1247-1257.

[24] Rajamäki, J. "Resilience Management Concept for Railways and Metro Cyber-Physical Systems," in *Proceeding of the 20th European Conference on Cyber Warfare and Security ECCWS*, T. Eze, Ed., Reading, Academic Conferences International Limited, 2021, pp.337-345.

[25] National Security Authority of Finland, *KATAKRI 2020 Information Security Audit Tool for Authorities*, National Security Authority, Helsinki, 2020.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

Niroj Chaulagain, Markus Kukkonen, Pessi Nurmi, Mikko Honkonen, Samu Saarinen, and Torsti Kinnunen collected the research data, made a preliminary analysis, and tentatively wrote Sections 3 and 4.

Jyri Rajamäki defined the purpose of the study, research questions, and methods, supervised the work, and finalized the report.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

This work was supported by the DYNAMO project, which has received funding from the European Union's Horizon Europe research and innovation funding program under grant agreement no. 101069601.

Conflict of Interest

The authors have no conflicts of interest to declare.