LOCKing Patient Safety: A Dynamic Cybersecurity Checklist for Healthcare Workers

Jyri Rajamäki, Kimberley Wood and Benjamin Espada
Laurea University of Applied Sciences, Espoo, Finland

Jyri.Rajamaki@laurea.fi
Kimberley.Wood@student.laurea.fi
Benjamin.Espad@student.laurea.fi

Abstract: Ensuring the cybersecurity of patient data is particularly challenging for healthcare organizations, and healthcare professionals play a key role here. Therefore, they must have the necessary knowledge and skills to be able to identify cybersecurity risks and respond appropriately to them. As part of the CyberSecPro project, this work-in-progress paper aims to provide healthcare professionals with a simple and memorable cybersecurity checklist highlighting important factors to consider. The purpose of the checklist is to support busy healthcare workers in implementing effective cybersecurity measures to secure sensitive information and guarantee patient privacy. The interview method was used to find out the cybersecurity challenges faced by healthcare workers and gather their opinions into a checklist. The mini-mental cybersecurity checklist created in the study, emphasizes the importance of being aware of cyber threats and maintaining secure and reliable information systems. Its name "LOCK" stands for Logging Out every time you leave your computer, Checking e-mails before opening links, and Keeping safe. Keep calm and LOCK on.

Keywords: Cybersecurity, Checklist, Data protection, Digital healthcare, Safeguarding

1. Introduction

Technology is increasingly becoming integral to healthcare facilities in today's healthcare landscape. Technology integration in healthcare offers significant benefits. This also exposes medical devices and healthcare systems to cybersecurity vulnerabilities, making them more vulnerable to cyber threats. Traditional notions of healthcare systems being immune to cyberattacks are no longer valid (Zhuravlev & Blagoveshchenskaya, 2020). The healthcare industry is facing critical cybersecurity issues resulting in patient data breaches (Cartwright, 2023). Delayed detection of cyber threats exacerbates this vulnerability, making it essential to address the issue of inadequate cybersecurity in the healthcare sector (Sabra, 2021). Inadequate investments and training have left the sector vulnerable to cyberattacks. Hacking, mainly through malware and ransomware, compromises patient data and causes disruptions to health services. These breaches lead to financial losses, damage healthcare institutions' reputations, and endanger patient safety (Kandasamy et al., 2022). Therefore, taking immediate action to secure these systems and devices to protect against potential attackers has become crucial. It is crucial to adopt a security-conscious approach integrated with patient care practices.

The CyberSecPro project, funded by the European Union, creates cutting-edge education and training materials and courses to advance competencies and professionalism in EU cybersecurity. Its goal is to strengthen the role of higher education institutions as a provider of practical and working life skills to promote reliable digital change in the critical sectors of health, energy, and transport. CyberSecPro aims to promote cybersecurity education in the following ways: (1) development of material for the development of theoretical and practical skills, (2) training and certification of students and professionals, and (3) promotion of partnerships (CyberSecPro, 2023).

This work-in-progress paper aims to develop material for improving healthcare professionals' theoretical and practical skills in the field of cybersecurity. The paper explores methods for developing a simple and memorable cybersecurity checklist that nurses can use to enhance cybersecurity in the healthcare industry. It also aims to identify the essential factors that should be considered while creating a cybersecurity checklist that is easy and convenient for busy healthcare workers to remember and use efficiently.

2. Methodology

Figure 1 shows how the Design Science Research (DSR) framework (Hevner & Chatterjee, 2010) is applied in this paper. The purpose of the research is to develop a simple and memorable cybersecurity checklist that healthcare professionals can use to enhance cybersecurity. The Relevance Cycle connects the contextual healthcare environment to the design science activities and the research problem of developing material for improving healthcare professionals' theoretical and practical skills in the field of cybersecurity. The healthcare domain consists of people (e.g., healthcare professionals, patients, clients, system operators, and security officers), and organizational and technical systems (e.g., eHealth infrastructure, patient data repositories) that interact to

work toward a goal. The Rigor Cycle combines the scientific foundations, experience, and expertise of design science with the Knowledge Base database. The central Design Cycle iterates between the core activities of building and evaluating the design artifacts and processes of the research. In this DSR, the evaluation is done as a desk study.

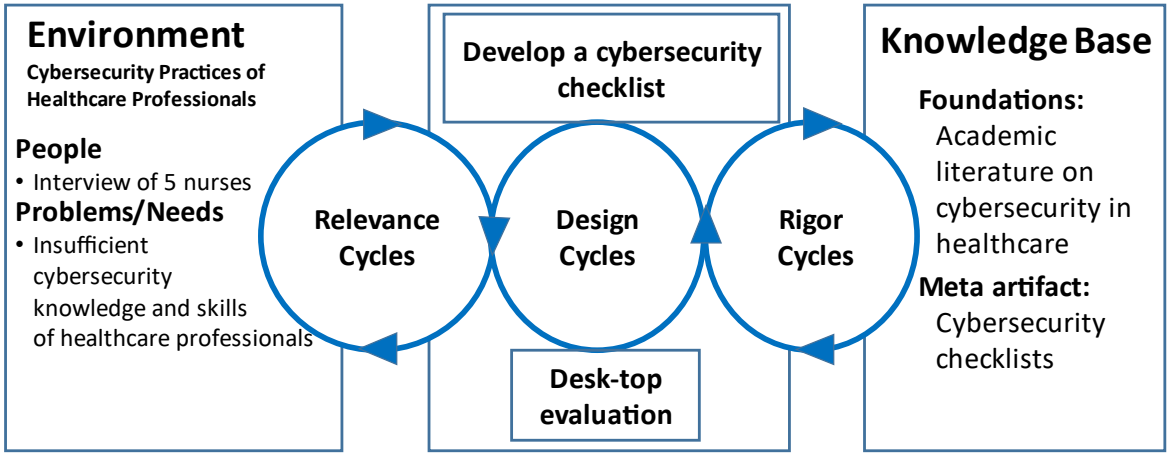

Figure 1: Design Science Research framework of this study

As a part of the relevance cycle, we selected five respondents with expertise in healthcare cybersecurity through convenience sampling. We conducted semi-structured interviews to gain insights into cybersecurity practices, challenges, and strategies. During the rigor cycle, we conducted a literature review that revealed significant risks to patient data and operational continuity in healthcare cybersecurity.

3. Rigor Cycle

3.1 Cybersecurity Practices of Healthcare Professionals

The healthcare industry is a primary target for cyberattacks, resulting in many data breaches. These attacks can be catastrophic for patients, healthcare providers, and the healthcare system. They can cause the loss of sensitive patient data, financial losses, and even patient harm. Although technology integration has led to greater precision in healthcare, cybersecurity measures must advance to keep up with the changes (Pant et al., 2022). On the other hand, only 22.7% of the non-ICT personnel (i.e., doctors, nurses, auxiliary, laboratory, and administrative personnel) felt sufficiently trained in security (Gioulekas et al., 2022).

Healthcare professionals are highly vulnerable to cybersecurity threats as they handle sensitive patient information and rely heavily on technology for various aspects of their work (Pant et al., 2022). The likelihood of medication errors increases if prescription systems do not work (Altamimi, 2022). Among healthcare professionals, nurses are often responsible for collecting and recording patient data, communicating with other healthcare professionals, and accessing electronic health records (Pant et al., 2022). Therefore, they must take proactive measures to implement robust cybersecurity practices to safeguard patient information and prevent data breaches. By doing so, healthcare professionals can ensure that patient data remains secure and prevent unauthorized access or theft of sensitive information.

Identifying phishing messages is crucial. As illustrated by an Italian hospital boasting a workforce of over 6,000 healthcare professionals, conducting an annual phishing simulation is integral to their training and risk assessment protocols (Rizzoni, et al., 2022). Employees play a pivotal role in fortifying the security of both the healthcare organization and patients' privacy by remaining vigilant towards suspicious emails, including scrutinizing links and attachments. Employees must exercise caution with unexpected emails and develop the ability to discern dubious messages, refraining from opening any associated attachments. Indiscriminate opening of email attachments should be strictly avoided. Recognizing one's activities and skills, particularly when under stress, is of paramount importance. The likelihood of human errors rises in demanding conditions and when departing from the established workflow (Sütterlin, et al., 2022). Stressed healthcare professionals are more susceptible to falling victim to phishing emails. Notably, there exists a clear positive correlation between the workload of nurses and the occurrence of opening phishing messages. Regrettably, healthcare personnel may be unaware of the potential consequences of their actions and the associated risks. The staff may not

comprehend that their behavior could facilitate the entry of malware into the hospital's system (Rajamäki, Rathod & Kioskli, 2023).

3.2 Cybersecurity Checklist

Preventing cybersecurity breaches in the healthcare industry can be achieved in several ways. One practical approach involves investing in risk management systems that detect and address potential cybersecurity risks. Another crucial aspect of cybersecurity is personnel's cybersecurity awareness (Gioulekas et al., 2022). This can be improved by ensuring that healthcare professionals receive adequate training to recognize and respond to cyber-attacks. These training programs should focus on educating healthcare professionals about the various types of cybersecurity threats they may encounter, how to identify possible signs of an attack, and the appropriate actions to take in response (Nifakos et al., 2021).

Implementing a cybersecurity checklist can significantly reduce the risk of cybersecurity breaches. Studies have shown that checklists can enhance patient safety and minimize errors in healthcare facilities. In addition, utilizing a checklist can ensure that healthcare professionals are adhering to the proper cybersecurity protocols (Wen et al., 2021). A well-defined software update procedure can help ensure systems are regularly patched and safeguarded against known vulnerabilities. Checklists have been successfully implemented in various industries, such as aviation and surgery, and there is potential for them to be utilized in the healthcare sector as well (Rêgo, 2019).

4. Relevance and Design Cycles

The interviews with Nurses A, B, C, D, and E revealed that patient data privacy is their topmost priority in healthcare practice. They all agreed that sensitive patient information should be safeguarded, and phishing emails should be prevented as they pose a common threat to healthcare professionals. When it comes to addressing cybersecurity concerns, Nurses A, B, C, and E mentioned that they rely on hospital-organized training sessions and updates from the IT department. On the other hand, Nurse D emphasized the importance of annual cybersecurity training sessions and online resources provided by the IT department.

All nurses suggested including verifying email sources, creating robust passwords, and identifying suspicious activities on devices in a cybersecurity checklist. They also recommended adding contact information for reporting incidents and an overview of prevalent healthcare-related cybersecurity threats. To make the checklist more engaging and user-friendly, Nurses A, B, D, and E proposed using visual aids and real-life examples. Nurse B suggested implementing regular reminders and easy access through technology such as an app or QR codes. Nurse C suggested enhancing engagement through interactive training sessions.

Despite recognizing time constraints as a significant obstacle, all nurses emphasized the importance of having concise and easily accessible checklists on workstations (Teng et al., 2021). They believe that a checklist would be a handy reminder to follow cybersecurity best practices, especially with busy schedules. These insights highlight the need for accessible, engaging, and concise cybersecurity resources to help healthcare professionals effectively address cybersecurity challenges daily.

The cybersecurity checklist produced in this study, tailored for the healthcare sector, includes the following three key elements:

1. Log Out - Logging out of computer systems and applications is a fundamental practice in cybersecurity. Logging out of users is important as a preventive measure against unauthorized access to patient data. Educating users has a positive effect on improving logout compliance.
2. Check Emails - Phishing attacks are a common entry point for cyber threats. Krause (2017) investigates the effectiveness of email security awareness training in healthcare settings. Their findings reveal that training programs significantly reduce the likelihood of healthcare professionals falling victim to phishing emails, enhancing email security.
3. Keep Safe - Securing devices and data is essential in healthcare cybersecurity. Nifakos et al. (2021) examine the role of encryption in securing patient data on portable devices. Their research underscores the importance of encryption practices and the need for continuous antivirus and anti-malware software updates.

5. Discussion

The purpose of this paper is to investigate ways to create a straightforward and easy-to-remember cybersecurity checklist that healthcare practitioners can use to improve cybersecurity in the healthcare sector. The goal is to determine the key factors to consider when designing a cybersecurity checklist that is user-friendly and convenient for busy healthcare workers to use effectively. By synthesizing information from various sources, we have identified three essential elements that should be included in a cybersecurity checklist for healthcare professionals: proper log-out procedures, email security awareness training, and device and data encryption.

Healthcare professionals should implement a comprehensive cybersecurity checklist specifically tailored to the healthcare industry (Poleto et al., 2021). By incorporating key elements such as logging out of computer systems and applications, checking emails for phishing attacks, and securing devices and data through encryption and regular updates, healthcare professionals can effectively mitigate cyber risks and threats. Moreover, healthcare professionals must be educated about the potential risks associated with cyber threats and the importance of proactively addressing them (Puder et al., 2023). To achieve this, policymakers and healthcare institutions must implement proper measures for cybersecurity, including investing in risk management systems and training employees to recognize and be vigilant against cyberattacks. While these measures may impact the speed of accessing patient information, it is a necessary trade-off to ensure the safety and security of sensitive data.

It is also essential to recognize the significance of ongoing user training programs in reinforcing these cybersecurity practices. Studies have shown promising results in improving compliance rates and reducing vulnerabilities. By prioritizing cybersecurity and integrating these practices into daily routines, healthcare professionals can contribute to developing a robust "human firewall" that safeguards patient information and promotes a culture of cybersecurity within the healthcare industry (Nifakos et al., 2021). Implementing these cybersecurity measures is crucial for protecting the integrity and privacy of patient data and ensuring the continuity and quality of healthcare services. To address the existing gaps in cybersecurity training for healthcare professionals, it is imperative to establish a standardized mode of delivery, a comprehensive curriculum, and clear training assessment criteria.

Using the checklist in healthcare settings can help healthcare professionals understand the importance of cybersecurity and take necessary steps to protect patient data and prevent cyberattacks (Dias et al., 2021). Furthermore, the checklist can serve as a valuable tool for healthcare institutions to assess their current cybersecurity practices and identify areas for improvement.

6. Conclusions

The healthcare industry suffers from a lack of awareness of cyber risks, even though understanding them and recognizing the effects of individual actions contributes significantly to the organization's overall cybersecurity. Nurses play a key role in protecting patients' data privacy. However, they have difficulties in ensuring cybersecurity measures. One significant way to improve cybersecurity in the healthcare industry is to provide nurses with enhanced awareness to practice cybersecurity behaviors. Based on the interviews conducted in this study, a checklist has been developed to provide user input and insights to improve cybersecurity.

In addition to focusing on nurses' cybersecurity practices, the literature emphasizes the importance of identifying the effects of cyber incidents. These effects are far-reaching and affect both the healthcare organization and its patients. Nurses' further training should also focus on dealing with the effects of cyber disruptions.

Acknowledgements

The research conducted in this paper was triggered by the project ‘Collaborative, Multi-modal and Agile Professional Cybersecurity Training Program for a Skilled Workforce In the European Digital Single Market and Industries’ (CyberSecPro) project. This project has received funding from the European Union’s Digital Europe Programme (DEP) under grant agreement No 101083594. Special thanks to the partners of these projects and their contributions.

References

Altamimi, S. (2022) "Investigating and mitigating the role of neutralisation techniques on information security policies violation in healthcare organisations", PhD thesis, University of Glasgow.

Cartwright, A. (2023) "The elephant in the room: cybersecurity in healthcare", *Journal of Clinical Monitoring and Computing,* Vol 1, No. 10.

CyberSecPro (2023) Home. [Online] Available at: https://www.cybersecpro-project.eu/ [Accessed 27 12 2023].

Dias, F., et al. (2021) "Risk management focusing on the best practices of data security systems for healthcare", *International Journal of Innovation,* Vol 9, No. 1, pp. 45-78.

Gioulekas, F., et al. (2022) "A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures", *Healthcare,* Vol. 10, 327. pp 1-19.

Hevner, A. & Chatterjee, S. (2010) *Design research in information systems: theory and practice*, New York: Springer Science and Business Media.

Kandasamy, K., Srinivas, S., Achuthan, K. & Rangan, V. (2022) "Digital Healthcare - Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST Perspectives, and Recommendations", *IEEE Access*, Vol. 10, pp. 12345-12364.

Kruse, C.S., Smith, B., Vanderlinden, H., et al. (2017) "Security Techniques for the Electronic Health Records", *J Med Syst,* Vol 41, 127.

Nifakos, Sokratis, et al. (2021) "Influence of human factors on cyber security within healthcare organisations: A systematic review", *Sensors* 21.15: 5119.

Pant, K., Bhatia, M., & Pant, R. (2022) "Integrated care with digital health innovation: pressing challenges", *Journal of Integrated Care* 30.4, pp. 324-334.

Poleto, T, et al. (2021) "Fuzzy cognitive scenario mapping for causes of cybersecurity in telehealth services", *Healthcare,* Vol. 9, No. 11.

Puder, A., Henle, J. & Sax, E. (2023) "Threat Assessment and Risk Analysis (TARA) for Interoperable Medical Devices in the Operating Room Inspired by the Automotive Industry", *Healthcare,* Vol. 11, No. 6.

Rajamäki, J., Rathod, P. & Kioskli, K. (2023) "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.

Rêgo, A. (2019) "WHO Surgical Safety Checklist", *Biomedical Journal of Scientific & Technical Research,* Vol. 20, No. 1, pp. 14815-14816.

Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M., & Coventry, L. (2022) "Phishing simulation exercise in a large hospital: A case study", *Digital Health* 8, 20552076221081716.

Sabra, M. (2021) "Cyberthreats on Implantable Medical Devices", *JISCR*, Vol. 4, No. 1, pp. 36-42.

Sütterlin, S., Knox, B. J., Maennel, K., Canham, M., & Lugo, R. G. (2022) "On the Relationship between Health Sectors' Digitalization and Sustainable Health Goals: A Cyber Security Perspective", *Good Health and Well-Being*, 133.

Teng, Z. et al. (2021) "Checklist Usage in Secure Software Development", In: David C. Wyld et al. (Eds) *Computer Science & Information Technology (CS & IT),* pp. 283-293.

Wen, X., et al. (2021) "Systematic Evaluation of the Effect of Bedside Ward Round Checklist on Clinical Outcomes of Critical Patients", *Journal of Healthcare Engineering* 2021.

Zhuravlev, M. & Blagoveshchenskaya, O. (2020) "Telemedicine: current state and COVID-19 lessons", *Legal Issues in the digital Age* 2: 92-143.