Demand Analysis of the Cybersecurity Knowledge Areas and Skills for Nurses: Preliminary Findings

Jyri Rajamäki [1], Paresh Rathod [1] and Kitty Kioskli [2]
[1] Laurea University of Applied Sciences, Espoo, Finland
[2] trustilio B.V, Amsterdam, The Netherlands

jyri.rajamaki@laurea.fi
paresh.rathod@laurea.fi
kitty.kioskli@trustilio.com

Abstract: The purpose of this paper is to present a preliminary analysis of the cybersecurity market demand in the nursing and health sector. Currently, the market demand study is ongoing under the Digital Europe Programme CyberSecPro project, which strengthens the role of higher education institutions as a provider of practical and working life skills. The project promotes reliable digital transformation in critical sectors, such as healthcare. The rapid development of e-health emphasizes the central position of cybersecurity in healthcare organizations that are increasingly the targets of cyber-attacks. This descriptive literature review explores what a nurse needs to know about cybersecurity. Our results show that awareness of cyber risks is weak in the healthcare sector. Understanding cyber risks and recognizing the effects of one's own activities increases the cybersecurity of the entire organization, therefore cybersecurity training for nurses should be increased. Our study suggested that nurses' most important cyber skills are their own cyber-safe way of operations, identifying cyber threats related to equipment, identifying the effects of cyber disruptions, and acting in a cyber disruption situation. Future nurse training programs should be updated to include these skills. Additionally, the teaching of nurses must be developed so that it meets these competence needs.

Keywords: cybersecurity skills, cybersecurity in healthcare, nursing competence, cybersecurity education, cybersecurity training

1. Introduction

As the healthcare sector continues to offer life-critical services while working to improve treatment and patient care with new technologies, criminals and cyber threat actors look to exploit the vulnerabilities that are associated with these changes. Among the most significant cyber-attacks from over the last 5 years are Anthem Blue Cross (78.8 Million Affected), American Medical Collection Agency Data breach (25 Million Patients Affected), Premera Blue Cross (11 Million Affected), Excellus BlueCross Blue Shield (10 Million Affected), and University of California, Los Angeles Health (4.5 Million Affected) (Stoianov & Bozhilova, 2019). So, it is crucial for all healthcare professionals to know how to manage their work in a cyber-secure manner and understand the effects cyber-attacks can have on the healthcare system.

EU Higher Education Institutions (HEIs) have more than 128 cybersecurity academic programs (undergraduate and graduate) as identified by ENISA (CYBERHEAD), JRC (ATLAS), and a variety of reports by the 4 pilot projects (Sparta, CyberSec4Europe, ECHO, CONCORDIA). The academic programs must offer dynamic capabilities and emerging skills that are required in the market to meet the demands for the cybersecurity workforce and expertise. The digital transformation imposes the HEIs to enhance their role in preparing the new generation workforce and to upskill-reskill the existing one in meeting the challenging and ever-growing cybersecurity challenges. Seventeen HEIs and thirteen security companies from sixteen European countries launched the agile CyberSecPro professional cybersecurity practical and hands-on training program that will complement, support, and advance the existing academic programs by linking innovation, research, industry, academia, and SME support. CyberSecPro aims to bridge the gap between degrees, working life, and marketable cybersecurity skill sets necessary in digitalization efforts and become the best practice for all cybersecurity training programs (see Figure 1).

This paper aims to present a preliminary analysis of the market demand for cybersecurity in the nursing and health sector. The ongoing market demand study is part of the CyberSecPro project under the Digital Europe Programme, which focuses on empowering higher education institutions to provide practical and relevant skills for the workforce. This paper also highlights the relevance of the CyberSecPro project in the context of the healthcare sector. In the future, this paper will provide more in-depth insights and report specific outcomes from the ongoing research and innovation work being conducted as part of the CyberSecPro Digital Europe Programme project. Further, CyberSecPro aims to pilot the European Cybersecurity Skills Framework in practice for cybersecurity professional training.

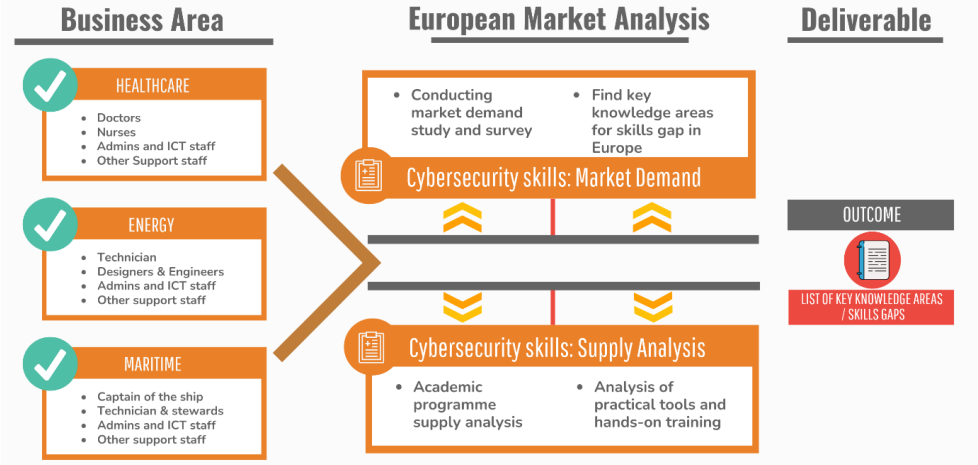

Figure 1: Market analysis of cybersecurity knowledge areas and skills [Source: Rathod & Polemi (2022)]

2. Methodology and collection of research material

The descriptive literature review (Paré et al., 2015) summarizes the most recent empirical research and answers the research questions about *what nurses should know about cybersecurity* and *what cyber skills/competencies they should have*. This work-in-progress paper used Google Scholar as the database. Four different search expressions formed with the Boolean operator were used from the selected search words. Only articles and research reports published in 2022 were considered. Table 1 shows the search results and how many of these are openly available in full text.

Table 1: Search expressions and results

Search expression	Search result documents	Open availability
nurse AND competence AND “cybersecurity in health care”	2	2
nurse AND competence AND “cybersecurity in healthcare”	6	3
nurse AND competence AND “cybersecurity in health care”	5	1
nurse AND competence AND “cybersecurity in healthcare”	52	20

We read the abstracts of 26 articles/research reports that met the search criteria and assessed whether they could find answers to the research questions. Table 2 shows six documents that, based on their abstracts, were selected for closer examination and analyzed using qualitative content analysis (Elo, et al., 2014).

Table 2: Selected articles

Articles/research report	Type	Subject area
Altamimi (2022)	Doctoral dissertation	Medical practitioners’ behavioral justifications
Gioulekas, et al. (2022)	Journal article	Personnel’s cybersecurity awareness
Isännäinen & Tulkki (2022)	Bachelor thesis (In Finnish)	Nurses’ know-how and skills
Rizzoni, et al. L. (2022)	Journal article	Personnel’s cybersecurity training
Sütterlin, et al. (2022)	Book chapter	Human factors
Wasserman & Wasserman (2022)	Journal article	Personnel’s cybersecurity training

In addition, the paper presents the preliminary findings of the Market Demand component of the CyberSecPro project, which falls under the larger Digital Europe Programme. This project aims to enhance the position of higher education institutions as a source of pragmatic and career-oriented competencies, with a particular emphasis on cybersecurity. These early results shed light on the project's initial stages and demonstrate its potential to positively impact the field of cybersecurity education for the nursing and other critical sectors.

3. Results

This paper presents the preliminary findings of an ongoing survey aimed at assessing the current market demand for cybersecurity skills, competencies, knowledge areas, and job roles. The survey focuses specifically on the nursing and health sector and aims to identify the top 12 most critical areas of cybersecurity knowledge required in this field. Based on the initial results of the survey, the following areas were found to be the most important and relevant for the nursing and health sector. It is noteworthy that Risk Management remains the most important and crucial knowledge area.

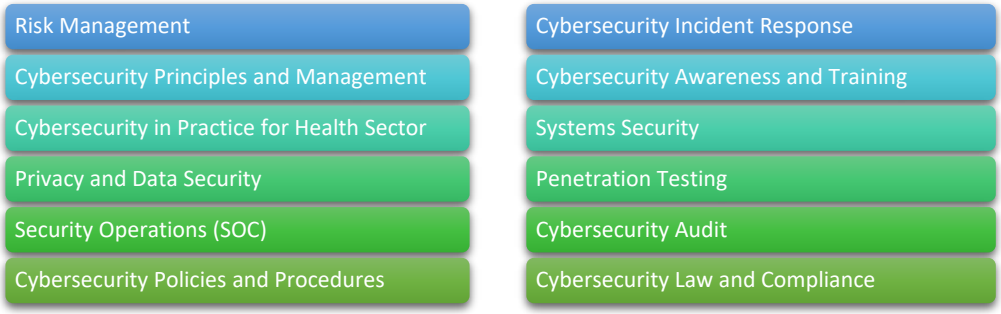

Figure 2: The Most Important Cybersecurity Knowledge Areas for Health and Nursing Sector: CyberSecPro Market Demand Early Outcomes

The further market demand analysis needs more careful data analysis and will be reported in the future long paper that would include the skills, competencies, and job roles. This paper also presents the results of the systematic literature studies.

The results of the qualitative content analysis are reported here according to the 5-step resilience cycle (see Figure 3). In the preparation phase, the nurse's most important skill is to be aware of cyber threats and their effects. In the prevent and protect phases, the most important thing is the cyber-safe operation of the nurse. In the response and recovery phases, the nurse must know how to act in a cyber disruption situation.

3.1 Analyzing and Identifying - Cyber threats and impacts

According to Gioulekas, et al. (2022), only 22.7% of the non-ICT personnel (i.e., doctors, nurses, auxiliary, laboratory, and administrative personnel) felt sufficiently trained in security, while only 38.5% were confident they could recognize a security issue or incident if they encountered one. Identifying the effects of cyber disturbances consists of the effects of cyber disturbances on the patient, the effects of cyber disturbances on the nurse's work, the effects of cyber disturbances on the operation of the hospital, and the effects of cyber disturbances on the medical device (Isännäinen & Tulkki, 2022). As a result of disturbances, the treatment of patients may be compromised in many ways. The likelihood of medication errors increases if prescription systems do not work, or a password is shared illegally (Altamimi, 2022). Stolen personal data are good and long-term investments for cybercriminals, which are used to acquire medicines and devices that are sold on the black market. Personal data is also used to make fake insurance claims. Cyber disruptions are not only a threat to patients' identities, but they can delay or disrupt hospital operations, putting patients' health and well-being at risk. The effects of cyber disruptions directly on the health and safety of patients and the functionality of medical devices. The WannaCry and NotPetya ransomware serve as examples of the deterioration of healthcare performance, as they hindered the operation of implantable heart devices, among other things. The probability of treatment errors increases when the hospital's information and equipment systems are damaged through cyber-attacks. Cyber-attacks are life-threatening crimes because the entire operation of the hospital must be stopped as a result of a cyber-attack at worst, being a big patient safety risk. Cyber-attacks can also affect other critical systems for the hospital, such as heating, ventilation, and air conditioning. These affect not only the patient but also the operation of the hospital and thus directly the nurse's ability to work.

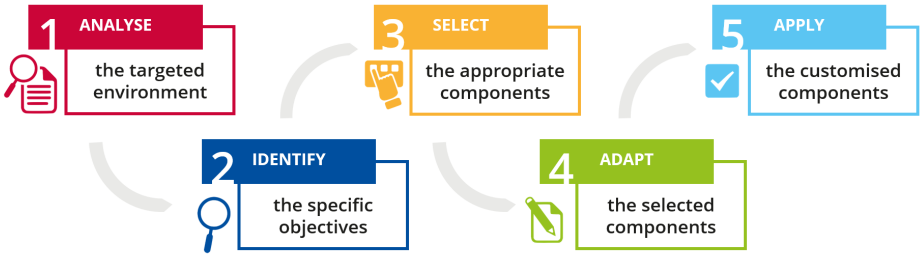

Figure 3: The 5-step resilience cybersecurity application [Source: European Cybersecurity Skills Framework]

Both medical devices and external devices carry risks. The risks of cyber-attacks related to external devices have increased. In the work of a nurse, risks are caused by the use of USBs and personal devices. Both staff and visitors use USB sticks on hospital machines, and anti-virus does not automatically prevent the spread of malware (Isännäinen & Tulkki, 2022). The risk of cyber-attacks increases as hospital equipment increasingly networks with external devices. The staff experiences challenges with devices connected to the Internet. Many nurses do not feel that they are sufficiently prepared or trained to use these devices. However, medical devices may be less at risk than other hospital devices, as hacking medical tools requires basic skills and knowledge of such specialized devices and often an understanding of the clinical implications of device changes (Wasserman & Wasserman, 2022).

3.2 Selecting - The cyber-safe operation of a nurse

Nurses' cyber-safe operation consists of their computer and ICT skills as well as the identification of various risks. The starting point of a nurse's activities with computers is that (s)he knows how to use the ICT operating environment created by ICT professionals in the best possible way.

Identifying the risks associated with usernames and passwords is important. Employees can increase the security of the organization and patients by paying attention to passwords and their use. The workplace password may not be used elsewhere, it may not be written down and it may not be shared with other employees. Double log-in policy, when the same username is logged in on 2 different computers, a security information reminder, and an instruction message should appear to remind the user, and it will require the account holder to log out from the initial session (Altamimi, 2022). The password must not be shared on the phone, which is also partly related to the identification of phishing. The password itself must not contain identifiable information. A strong password created within the limits defined by the organization must be used. Passwords should not be repeated or written down. The use of automatic login and remember me functions on workstations also carries risks. Although sharing passwords may seem like a factor that makes work run smoothly for employees, the unauthorized use of passwords can even be interpreted as criminal activity.

Phishing messages should be recognized. For example, a large Italian hospital with over 6,000 healthcare workers conducts a phishing simulation as part of its annual training and risk assessment (Rizzoni, et al., 2022). Employees can increase the security of the organization and patients by paying attention to suspicious e-mails and their links and attachments. The employee must be considerate when it comes to unexpected emails and learn to recognize suspicious messages. These attachments should not be opened. Random and thoughtless opening of e-mail attachments should be avoided. Recognizing the nurse's own activities and skills, even when under load, is important. Human errors increase in demanding conditions and when deviating from the traditional way of working (Sütterlin, et al., 2022). A stressed nurse is also more likely to open phishing emails. There was a clear positive correlation between nurse workload and opening phishing messages. Healthcare personnel does not know what consequences their behavior may have and what risks it may cause. The staff is not aware that their own actions may contribute to the malware's entry into the hospital's system.

The cybersecurity breaches observed in hospitals are often related to the low cybersecurity awareness of the staff (Gioulekas, et al., 2022). Personnel does not know the consequences of their behavior and they are often only trained further after a cyber-attack has already occurred. Identifying cyber risks is helped by understanding the goal of cyber-attacks. Hackers' main goal is usually not to harm patients but to gain access to the hospital's data network. However, hackers are also interested in patients' individual health and personal information, which usually remains unchanged. These include, for example, blood group, surgeries performed, and social security number. This information ending up in the hands of outsiders always causes a security breach.

Remote work increases the risks of a nurse's work. The studies state that employees were willing to do remote work, even though they are aware of the risks it makes possible. Also, risks associated with using social media applications exist. Although communication channels such as WhatsApp are fast and convenient, they can pose security risks (Altamimi, 2022).

3.3 Adapting and applying - Acting in a cyber disruption situation

A cyber disruption situation may lead to an emergency. In the event of a cyber-disruption, the nurse may not have access to information important to the patient's care. When a cyber-attack is detected, the entire hospital ICT system often must be shut down. The nurse, therefore, must rely on paper-based systems because computer-based systems are down (Isännäinen & Tulkki, 2022).

4. Discussion

Awareness of cyber risks is weak in the healthcare sector (Gioulekas, et al., 2022). Understanding cyber risks and recognizing the effects of one's own activities increases the cybersecurity of the entire organization. For this reason, nurses should be trained more in cyber-safe working. Along with the nurse's cybersecurity activities, the importance of identifying the effects of cyber disturbances emerged from the material. The effects are wide-ranging and affect the entire healthcare organization as well as the patients. Compliance with the security policy improves when medical professionals are involved in the development of cybersecurity practices (Altamimi, 2022). As a follow-up study, the literature research should be expanded into a systematic review over a longer period and from more databases. Further the study will also include more comprehensive market demand analysis. The market demands would be useful to find out the experiences and methods of operation related to cybersecurity from professionals and students in the field. The continuing education needs of nurses already at work should also be clarified.

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) programme under grant agreement No 101083594. Special thanks to the partners of these projects and their contributions. The third author (KK) would also like to acknowledge the project 'A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures' (AI4HEALTHSEC) under grant agreement No 883273. The sole responsibility for the content of this paper lies with the authors. The authors are grateful for the financial support of these projects that have received funding. The views expressed in this paper represent only the views of the authors and not of the European Commission or the partners in the above-mentioned projects.

References

Altamimi, S. (2022). Investigating and mitigating the role of neutralisation techniques on information security policies violation in healthcare organisations. https://theses.gla.ac.uk/82646/1/2022altamimiphd.pdf

CyberSecPro Innovation Project, European Union's DIGITAL-2021-SKILLS-01 Programme under grant agreement no. 101083594 (2022)

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative content analysis: A focus on trustworthiness. SAGE open, 4(1), 2158244014522633. 10 DOI: 10.1177/2158244014522633

European Union Agency for Cybersecurity. (2022). ECSF, European cybersecurity skills framework. Publications Office. https://doi.org/10.2824/859537

Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., ... & Ntanos, C. (2022). A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. *Healthcare* Vol. 10, No. 2, p. 327 https://www.mdpi.com/2227-9032/10/2/327/pdf

Isännäinen, A., & Tulkki, S. (2022). Kyberturvallisuus terveydenhuollossa: mitä sairaanhoitajan tulee tietää ja osata? [Cyber security in health care. What should a nurse know?] https://www.theseus.fi/bitstream/handle/10024/755584/Isannainen_Tulkki.pdf?sequence=2

Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. Information & Management, 52(2), 183–199. https://doi.org/10.1016/j.im.2014.08.008

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 https://journals.sagepub.com/doi/pdf/10.1177/20552076221081716

Scharte, B., Hiller, D., Leismann, T. & Thoma, K. (2014). Summary. In: *Thoma K (ed) Resilien Tech. Resilience by Design: a strategy for the technology issues of the future (acatech STUDY*). Herbert Utz Verlag, München, pp 117–125

Stoianov, N. & Bozhilova, M. (2019). D2.1 Sector scenarios and use case analysis, ECHO, 31 October 2019.

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. In: *Good Health and Well-Being*, 133 https://library.oapen.org/bitstream/handle/20.500.12657/59127/1/%5BHBK%5D%20Final%20Binder%20196%20pgs.pdf#page=151

Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Digital Health*, 135 https://www.frontiersin.org/articles/10.3389/fdgth.2022.862221/pdf