MODULE 2: DIGITAL SAFETY/ CYBERSECURITY IN HEALTHCARE

Tiina Blek and Jaana Mäkelä. School of Social and Health Studies, Jamk University of Applied Sciences

Introduction

Hospitals worldwide are becoming increasingly dependent on hospital information systems —with the use of connected medical devices, cloud storage services, and network systems simultaneous rising. Cybercrime against healthcare organizations is on the rise. Cyberattacks have become an international threat to patient care and safety. Attacks negatively impact access to healthcare services and challenge healthcare organizations to protect the confidentiality and integrity of health data (Argaw et al., 2019). The economic impact is significant. Median cost of a major security incident in the health sector is 300 000 Euro(European Union Agency for Cybersecurity (ENISA), 2022). Healthcare organizations are also forced to pay millions in breach costs. (Alder, 2023)

Access to the medical record system is described as a goldmine for cybercriminals. ID, insurance, billing, genetic and health data are data that cannot be changed as easily as credit card information. (Argaw et al., 2019) As a result, the value of health data on the dark web is 10 to 20 times greater than credit card data (Williams et al., 2020). Other reasons for cyber-attacks on healthcare systems include the large number of devices in use and outdated technology, medical devices that are easily accessible to cybercriminals (*9 Reasons Why Healthcare Is the Biggest Target for Cyberattacks*, n.d.).

It is estimated that 40-54 % of the cyber-attacks are caused by the healthcare worker's actions. Identified causes of insecure staff behavior are carelessness, rush, and lack of knowledge (2020 HIMSS Cybersecurity Survey, 2020). Repetitive tasks (routinisation) are risk factors (Jerry-Egemba, 2024), as well as attitudes towards security guidelines, external factors (e.g. social pressure), and employee's assessment whether the time and effort spent on security-related activities is worthwhile (Blythe John, 2013).

Coventry et al. (2020) find that reckless behavior related to information security is common in the health sector. Awareness of the extent of the risks associated with their own behavior is also often low. (Coventry et al., 2020) Factors influencing secure or, conversely, insecure behavior include attitudes towards security guidelines, external factors (e.g., social pressure), and an assessment of the risks associated with their own behavior and whether the time and effort spent on security-related activities is worthwhile. (Blythe John, 2013) Behavior is also influenced by the desire to rationalize and save time (Hedström et al., 2013) and often by a lack of knowledge and training in information and cyber security

Definition of main concepts of digital safety

Digital Safety or *Digital Security* is seen as a state where a digital operating environment can be trusted and operations related to it are secure and managed, even in the event of disruptions (Digital and population data services data agency, 2022). The OECD defines digital security as a broad concept, which includes digital security risk management, continuity management, data protection and information security and cybersecurity (OECD, 2022).

Cybersecurity refers to the security of a digital and networked society or organization and its impact on their operations. Cybersecurity includes measures to proactively manage and, if

necessary, tolerate various cyber threats and their effects (Digital and population data services data agency, 2022)

*Data protection includes a*rrangements, designed to ensure the fair processing of personal data and the preservation of privacy (The Finnish Terminology Centre, 2018).

Information security means arrangements that aim to ensure the availability, integrity and confidentiality of information. *Availability* is seen as a state where information is available when and where it is needed. *Integrity* refers to state where information is consistent with the original information, i.e. the information has not changed. *Confidentiality* means that no third party has access to the information. (Check Point, 2023)

Cyber Threats and Healthcare

In 2023, healthcare systems worldwide faced an average of 1,613 cyber-attacks per week. This represented an approximately 11% increase compared to the previous year. On average, about one in every 34 organizations across all sectors fell victim to ransomware attacks. The healthcare sector was the second most targeted, with one in every 25 healthcare organizations experiencing a ransomware attack. The highest number of ransomware attacks targeted government/military systems, affecting one in every 24 organizations (Figure 10). These attacks occur globally and are increasing annually. Cyber-attacks occur in small, medium, and large organizations. Attacks happen indiscriminately and negatively impact patient safety and staff operations, regardless of the organization's size, specialty, or other factors. (Check Point, 2023)

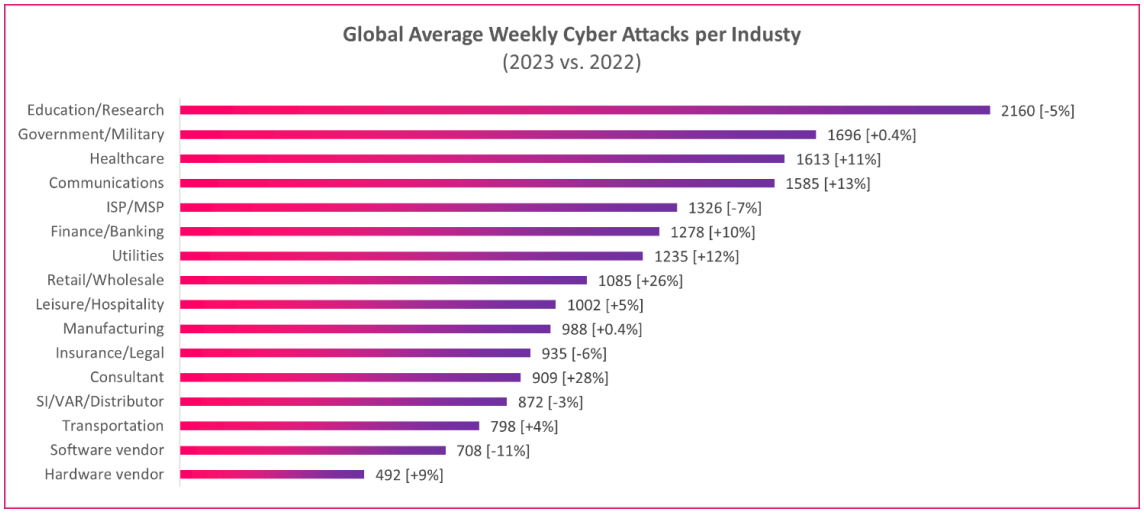

FIGURE 10. GLOBAL AVERAGE WEEKLY CYBER ATTACKS PER INDUSTRY. (CHECK POINT 2023.)

The most common cyber threats to healthcare information systems are data breaches, social engineering, ransomware**,** and denial of service (DoS) attacks. A *data breach* is an unauthorized interference with data or an information system. The most common types of security breaches

are misuse of user IDs and passwords, data breach and data theft. (Al-Qarni, 2023). The purpose of *social engineering* is to trick individuals or organizations into either revealing confidential information or downloading malicious activity onto a computer. The most commonly used distribution channel for phishing is email. (Nifakos et al., 2021) *Ransomware* is an attack that encrypts or manipulates data on a device and demands a ransom from the user to decrypt the data. A *denial-of-service attack* is an activity that loads and paralyses a network so that the service or information system no longer functions normally. (Al-Qarni, 2023).

There are also *attacks on medical devices*. Attacks can happen by tampering with a medical device with the intention of accessing data, changing settings, or using it as a gateway to access other systems. (Cartwright, 2023) Common cyber threats to healthcare are summarized in Table 3.

TABLE 3. COMMON CYBER THREATS TO HEALTHCARE. (JYVSECTEC, 2021)

CYBER THREAT	DESCRIPTION	EXAMPLES
PHISHING	Attacks aimed at obtaining confidential information by deceiving users.	Phishing emails related to work or personal life, Office 365 credential phishing.
MALWARE	Software that damages systems or data.	Emails spreading malware, ransomware that encrypts data.
DATA BREACHES	Unauthorized access to systems and theft of information.	Selling personal data and patient records, extortion through threats of data exposure.
DENIAL-OF-SERVICE ATTACKS	Attacks that disrupt or slow down system functionality.	Crashing systems, demanding ransom through threats of DDoS attacks.
CLOUD SERVICES	Vulnerabilities in cloud-based systems and services.	Incorrect system settings, denial-of-service attacks making data unavailable.
SOFTWARE	Weak security in the design and use of software.	Inadequate identity verification, vulnerabilities in coding, credentials exposed in user guides.
WIRELESS NETWORKS (WLAN)	Poorly secured wireless networks that allow eavesdropping or interference in communication	Unencrypted or weakly encrypted communication, manipulation of IoT devices.

MEDICAL DEVICES	Vulnerabilities and lack of updates in medical devices	Default factory settings not changed, vulnerabilities in infusion pumps, devices under remote monitoring by manufacturers.
REMOTE WORK	Security challenges related to remote work.	Potentially inadequate security, home environment increasing attack surface.
PHYSICAL ENVIRONMENT	Challenges in securing physical environments and risks of device contamination.	Device contamination through USB drives, loss or theft of information or devices.
PERSONNEL	Human errors and bypassing of security mechanisms.	Sharing of passwords, weak passwords, unintentional disclosure of patient information.

Risk Factors Related to Cybersecurity in the Healthcare Sector

Employee-Related Factors

- Repetitive Tasks (Routine): The nature of repetitive tasks in healthcare can lead to routine behavior, making employees less vigilant about cybersecurity threats (Jerry-Egemba, 2024).
- Burnout/Workload: High levels of burnout and heavy workloads are prevalent in the healthcare sector, contributing to decreased attention to cybersecurity measures (Clarke & Martin, 2024)
- Fatigue: Fatigue among healthcare workers can impair judgment and increase susceptibility to cyber threats (Jerry-Egemba, 2024).
- Fear and Uncertainty: The fear and uncertainty surrounding cyber threats can lead to anxiety and reduced effectiveness in managing cybersecurity (Cartwright, 2023).
- Social Isolation: Social isolation, particularly in remote work settings, can exacerbate feelings of vulnerability and reduce collaborative efforts to enhance cybersecurity (Cartwright, 2023).
- Lack of Knowledge: A significant gap in cybersecurity knowledge among healthcare workers can lead to inadequate responses to cyber threats (Kioskli et al., 2023).
- Unawareness of Personal Risk: Many healthcare workers do not recognize how their actions can contribute to cybersecurity risks (Kioskli et al., 2023).

- Spread of Information on social media: The rapid dissemination of information on social media can amplify the impact of cyber incidents (Nifakos et al., 2021).

Systemic and Technological Factors

- Global Underfunding of Healthcare: Chronic underfunding in the healthcare sector globally exacerbates vulnerabilities to cyber threats (Cartwright, 2023).
- Outdated Equipment: The use of outdated medical and IT equipment increases the risk of cyber-attacks (Clarke & Martin, 2024).
- Discontinuation of Support and Updates: The cessation of support and updates for older systems leaves them more vulnerable to cyber threats.
- Limited IT and Cybersecurity Personnel: A shortage of dedicated IT and cybersecurity staff in healthcare settings hampers effective threat management.
- Insufficient Training for Healthcare Staff: Inadequate training in cybersecurity for healthcare personnel leads to poor handling of cyber incidents.
- Emerging Targets for Cybercrime: New targets such as telehealth, remote care, and electronic consultations are increasingly exposed to cyber threats (Clarke & Martin, 2024).

By addressing these risk factors, the healthcare sector can enhance its resilience against cyber threats and protect both patient safety and sensitive information.

Impact of cyber-attacks on patient safety and staff

A cyber-attack has wide-ranging implications for the organization's operations, patient safety and the work of staff. One important impact is also the economic impact. The effects of cyber-attacks concern all staff groups within an organization (managers, IT staff, clinical staff, office services, etc.).

The effects of cyber-attacks on patient safety and staff operations depend on the type of attack (e.g., ransomware vs. data breach).)

Common impacts include:

1. Inaccessibility of patient records.
2. Disruption of treatment instructions.
3. Unavailability of patient medical history and health information.
4. Inaccessibility of medication information.
5. Limited or no access to laboratory and imaging results.
6. Restricted or unavailable use of medical devices.

7. Inaccessibility of email.
8. Unavailability of network connections.

In May 2021, the Irish public health service faced a cyber-attack, leading to the shutdown of ICT systems. This affected various services, including radiology, diagnostics, and oncology, and recovery took over four months. Moore et al. (2023) studied the short- and long-term effects of this attack. The study found that health service staff showed resilience and adaptability, quickly developing innovative solutions to ensure patient safety and service continuity. The attack placed significant stress on staff, exacerbating the already high stress levels from the COVID-19 pandemic. Concerns about long-term consequences for staff wellbeing were raised. There were also positive impacts as the attack led to a flattening of the healthcare hierarchy, empowering frontline workers. (Moore et al., 2023)

Cyber-attacks targeting medical devices have been reported, including incidents involving blood gas analyzers, X-ray machines, and MRI machines. Attacks often cause disruption to patient care, which increases the risk of complications, affects patient outcomes, and causes an increase in patient mortality rates. Ponemon Institute surveyed 653 IT and IT security practitioners in U.S. healthcare organizations. Forty-three percent of respondents say the data loss or exfiltration incident had an impact on patient care. Of these respondents, 46 percent of respondents say it increased mortality rates and 38 percent say it increased complications from medical procedures. (Ponemon Institute, 2023) (Figure 11).

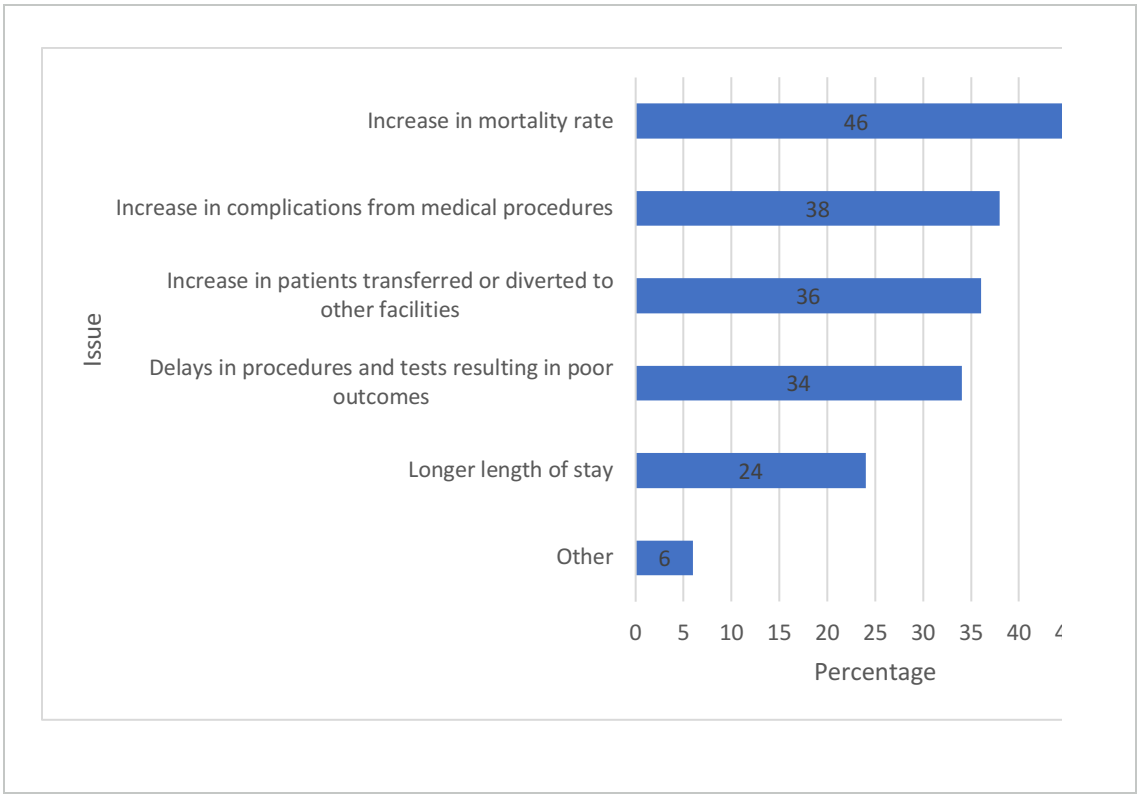

Figure 11. Impacts of the data loss or exfiltration incident on patient care. (Ponemon Institute, 2023)

The cybersecurity competence needs of healthcare staff

In the social and health care sector, cybersecurity skills are a topical issue that is increasingly seen as a competence need of every social care professional (Clarke & Martin, 2024a; Jerry-Egemba, 2024; Kioskli et al., 2023). Technological means can protect against cybercrime, but without an educated workforce and a strong security culture, an organization's protection falls short (Kamerer & McDermott, 2020).
A health care professional is not expected to understand codes or the technological aspects of using systems but should be able to act in a cyber-secure manner from the perspective of their role and professional responsibilities (Kamerer & McDermott, 2020; Rajamäki et al., 2023). Key competences also include recognizing cyber incidents and responding to them, as well as identifying cybersecurity threats related to various network-connected devices and equipment (Rajamäki et al., 2023).

In particular, healthcare professionals should have the following cybersecurity basics:

- Use strong passwords for all their accounts, including electronic medical record system. Passwords should be long and include a mix of uppercase and lowercase letters, numbers and special characters.
- Use only secure networks, such as workplace network or a trusted VPN, when accessing sensitive patient information or medical records.
- Avoid using public Wi-Fi networks or unsecured networks.
- Use secure messaging platforms to communicate with colleagues and other healthcare professionals.
- Avoid using unsecured messaging apps or SMS messages, which can be intercepted and read by unauthorized individuals.(Kioskli et al., 2023)

Identifying *social engineering* attempts (e.g. phishing) is a key area of cyber competence. (Kioskli et al., 2023) Every healthcare worker should have the ability to *detect abnormal activity* related to an information system, medical device or application and know how to react to such a situation. (Kamerer & McDermott, 2020). It is also important that staff using healthcare equipment and systems *identify the routes* through which a cyber-attack can spread to systems. (Dill, 2016). These critical gateways are workstations, copying machines, mobile devices, cloud-based applications, remote login, worker's own devices (USB, phone), open Wi-Fi and IoT devices such as medical/remote monitoring devices (Kioskli et al., 2023). An integral part of staff's tasks is to *guide patients* in the safe use of medical and telemonitoring devices. (Billingsley & McKee, 2016)
Cyber hygiene best practices for healthcare staff are described in figure one (Figure 12).

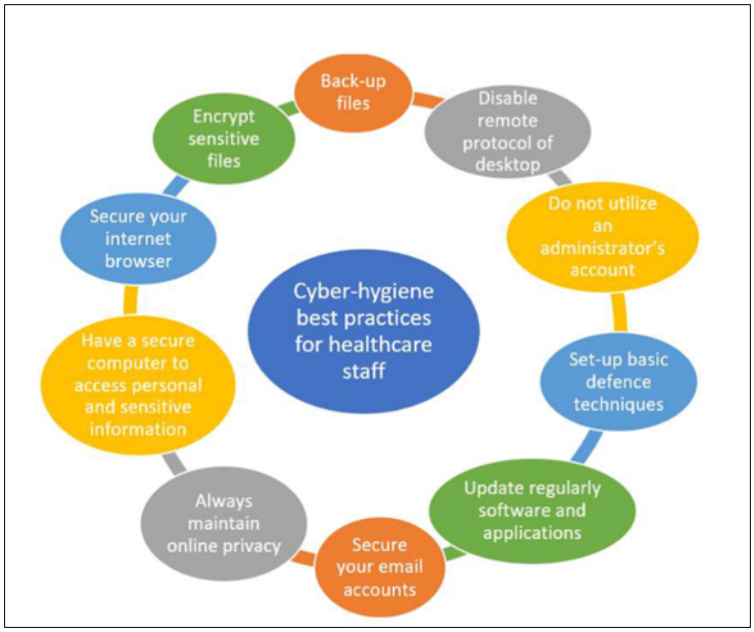

FIGURE 12. CYBER HYGIENE BEST PRACTICES FOR HEALTHCARE STAFF. (KIOSKLI ET AL., 2023)

Assessing the cybersecurity skills of health and social care staff is challenging. For example, staff may underestimate their competence because they do not fully understand what is meant by cybersecurity (Blek & Solankallio-Vahteri, 2022; Kannelønning & Katsikas, 2023). In a survey conducted for the HealthCare Cyber Range (HCCR) project, Blek & Solankallio-Vahteri (2022, 359) also find a discrepancy; 74% of healthcare professionals consider their cybersecurity knowledge to be at an adequate level. However, surveys, research evidence and cybersecurity incidents report the opposite (e.g. Coventry et al., 2020).

There are three key factors influencing healthcare workers' cybersecurity behaviour: 1) perceived barriers to efficiency and patient care, 2) lack of awareness of the consequences of behaviour, and 3) insufficient policies and reinforcement of safe behaviour (Coventry et al., 2020) In their study, Javaid et al. (2023) found that staff are more realistic in their assessment of their competence and more likely to follow cybersecure practices when they understand the importance of the practices and are aware of their role, threats, and factors that affect cybersecurity (Javaid et al., 2023).

Open and transparent communication between IT professionals and health and social care staff is crucial to fostering security awareness and culture (Clarke & Martin, 2024b). Involving staff in cybersecurity discussions and decision-making helps them understand guidelines and enables them to integrate security practices into clinical work (without slowing down the patient care process). In addition, involving staff in risk assessments, policy development and technology selection ensures that security measures are aligned with clinical work processes and effectively address staff concerns (Healthcare and Public Health Sector Coordinating Council, 2023).

References

9 reasons why healthcare is the biggest target for cyberattacks. (n.d.). Retrieved September 8, 2021, from https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/

2020 HIMSS Cybersecurity Survey. (2020).

Alder, S. (2023). 66% of Healthcare Organizations Say Patient Care was Disrupted by a Cyberattack. *TheHIPAAJournal*.

Al-Qarni, E. A. (2023). Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies. *International Journal of Advanced Computer Science and Applications*, *14*(5). https://doi.org/10.14569/IJACSA.2023.0140513

Argaw, S. T., Bempong, N.-E., Eshaya-Chauvin, B., & Flahault, A. (2019). The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. *BMC Medical Informatics and Decision Making*, *19*(1). https://doi.org/10.1186/s12911-018-0724-5

Billingsley, L., & McKee, S. A. (2016). Cybersecurity in the Clinical Setting: Nurses' Role in the Expanding "Internet of Things." *The Journal of Continuing Education in Nursing*, *47*(8), 347–349. https://doi.org/10.3928/00220124-20160715-03

Blek, T., & Solankallio-Vahteri, T. (2022). Terveydenhuollon hoitohenkilöstön tieto- ja kyberturvallisuusosaaminen. *Finnish Journal of EHealth and EWelfare*, *14*(4). https://doi.org/10.23996/fjhw.115829

Blythe John. (2013). Cyber security in the workplace: Understanding and promoting behaviour change. *Proceedings of CHI 2013 Doctoral Consortium*, 92–101.

Cartwright, A. J. (2023). The elephant in the room: cybersecurity in healthcare. *Journal of Clinical Monitoring and Computing*, *37*(5), 1123–1132. https://doi.org/10.1007/s10877-023-01013-5

Check Point. (2023). *2023 Cyber Security Report*.

Clarke, M., & Martin, K. (2024a). Managing cybersecurity risk in healthcare settings. *Healthcare Management Forum*, *37*(1), 17–20. https://doi.org/10.1177/08404704231195804

Clarke, M., & Martin, K. (2024b). Managing cybersecurity risk in healthcare settings. *Healthcare Management Forum*, *37*(1), 17–20. https://doi.org/10.1177/08404704231195804

Coventry, L., Branley-Bell, D., Sillence, E., Magalini, S., Pasquale, M., Magkanaraki, A., & Kalliopi, A. (2020, July 19). Cyber-risk in Healthcare: Exploring Facilitators and Barriers to Secure Behaviour. *HCI for Cybersecurity, Privacy and Trust: Second International Conference, HCI-CPT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19– 24, 2020,*

Digital and population data services data agency. (2022). *VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön – esittely ja johdatusta riskiviestintään*.

Dill, M. W. , L. S. & W. T. (2016). Understanding Cybersecurity: A Primer for HIM Professionals. *Journal of AHIMA*, *87*(4), 46–51.

European Union Agency for Cybersecurity (ENISA). (2022). *NIS INVESTMENTS*.

Healthcare and Public Health Sector Coordinating Council. (2023). *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*.

Hedström, K., Karlsson, F., & Kolkowska, E. (2013). Social action theory for understanding information security non-compliance in hospitals. *Information Management & Computer Security*, *21*(4), 266–287. https://doi.org/10.1108/IMCS-08-2012-0043

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, *1*, 100016. https://doi.org/10.1016/j.csa.2023.100016

Jerry-Egemba, N. (2024). Safe and sound: Strengthening cybersecurity in healthcare through robust staff educational programs. *Healthcare Management Forum*, *37*(1), 21–25. https://doi.org/10.1177/08404704231194577

JYVSECTEC. (2021). *A Handbook on Cyber Security Incident Response Processes for Healthcare Actors*.

Kamerer, J. L., & McDermott, D. (2020). Cybersecurity: Nurses on the Front Line of Prevention and Education. *Journal of Nursing Regulation*, *10*(4). https://doi.org/10.1016/S2155-8256(20)30014-4

Kannelønning, K., & Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. *Information & Computer Security*, *31*(4), 463–477. https://doi.org/10.1108/ICS-08-2022-0139

Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H. (2023). The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. *Applied Sciences*, *13*(6), 3410. https://doi.org/10.3390/app13063410

Moore, G., Khurshid, Z., McDonnell, T., Rogers, L., & Healy, O. (2023). A resilient workforce: patient safety and the workforce response to a cyber-attack on the ICT systems of the national health service in Ireland. *BMC Health Services Research*, *23*(1), 1112. https://doi.org/10.1186/s12913-023-10076-8

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors*, *21*(15), 5119. https://doi.org/10.3390/s21155119

OECD. (2022). *OECD Policy Framework on Digital Security*. https://doi.org/10.1787/a69df866-en

Ponemon Institute. (2023). *Cyberinsecurity in Healthcare:The Cost and impact on patient safety and care*.

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*, *22*(1), 711–716. https://doi.org/10.34190/eccws.22.1.1181

The Finnish Terminology Centre. (2018). *Vocabulary of Cyber Security*.

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity Risks in a Pandemic. *Journal of Medical Internet Research*, *22*(9), e23692. https://doi.org/10.2196/23692