Cyber Threats in Hospitals: GDPR and NIS2 Regulations in Preventing USB Injections

Ilkka Tikanmäki[1,2], Jyri Rajamäki[1], Forster Boateng, Jesse Kaikkonen, Batuhan Ketene, Joni Lehtiaho and Jussi Miestamo

[1]Security and Risk Management, Laurea University of Applied Sciences, Espoo, Finland
[2]Department of Warfare, National Defence University, Helsinki, Finland

ilkka.tikanmaki@laurea.fi
jyri.rajamaki@laurea.fi
batuhan.ketene@student.laurea.fi
forster.boateng@student.laurea.fi
jesse.kaikkonen@student.laurea.fi
joni.lehtiaho@student.laurea.fi
jussi.miestamo@student.laurea.fi

Abstract: Cybersecurity is crucial in healthcare due to the escalating use of digital technologies and the rise in cyber-attack risks. This research demonstrates the necessity for robust strategies to safeguard physical and digital infrastructures, ensuring the security of patient data and healthcare services. Healthcare providers can protect themselves from the prevalent cyber-attack risks by establishing robust security measures, protocols, and actions. The study aims to demonstrate the importance of aligning cybersecurity measures with the stringent regulatory demands of the General Data Protection Regulation (GDPR) and the Network and Information Systems Directive (NIS2). The security, privacy, and integrity of patient data within systems require a commitment to technical enhancements and procedural changes. Adhering to these regulations is not just obligatory, but also advantageous, as a secure information environment bolsters patients' confidence in the healthcare system. However, it is not easy to achieve a healthcare environment that is completely safe and compliant due to many challenges. Numerous challenges exist, such as enforcing uniform security measures across disparate systems and integrating new security technologies into legacy environments. The rising use of USB devices by healthcare staff has made hospital work areas more accessible to non-employees, including patients, their families, and students at university hospitals. Staff members may not fully comprehend the risks associated with using USB devices for exchanging clinical information. A virus infection in a portable USB device connected to Point of Care Testing (POCT) equipment can result in a partial denial of service. Navigating the complicated regulatory requirements adds to the complexity of this vital task. Although there are many obstacles, the proposed strategies provide a clear path to move forward. Organisations can fortify themselves against rising cyber threats by fostering a culture of continuous improvement and dedication, investing in the modernisation of outdated systems, and placing cybersecurity at the forefront of healthcare service delivery. This proactive approach is about safeguarding the core of healthcare, which is the health and safety of patients. The research question is: What vulnerabilities do USB devices introduce into healthcare systems, and how do they conflict with GDPR and NIS2 standards?

Keywords: Cybersecurity, POCT machines, health care, GDPR, NIS2

1. Introduction

The General Data Protection Regulation (GDPR) is a regulation by the EU intended to safeguard individual privacy and personal data for those within the European Union (European Parliament and the Council, 2016). It applies to entities that process the data of European Union (EU) residents, irrespective of where the organisations are located. The General Data Protection Regulation (GDPR) underscores the importance of transparency, fairness, and the legality of data processing activities (Wolford, 2018). The Network and Information Systems Directive (NIS2) is an EU-wide cybersecurity law that builds upon the original NIS Directive (European Parliament and of the Council, 2024). It establishes new obligations and requirements in four key areas: risk management, corporate accountability, incident reporting, and business continuity. NIS2 requires that essential and significant entities adopt fundamental security measures to counteract specific types of probable cyber threats.

In the healthcare sector, this translates to more stringent requirements for safeguarding patient data and preventing disruptions in health services. The fundamental security measures encompass conducting risk assessments, establishing security policies for information systems, implementing policies for cryptography usage, managing, and reporting vulnerabilities, setting security protocols for employees with access to sensitive data, and enforcing multi-factor authentication (MFA) (Cybersecurity & Infrastructure Security Agency, 2024).

In today's world, information has emerged as a highly valued asset across various organisations, particularly in the healthcare sector. The imperative for organisations to implement cybersecurity measures to safeguard

information and privacy has never been greater. Numerous instances of ransomware attacks on the healthcare sector have been reported. For example, (Mansfield-Devine, 2016) noted that half of the UK's National Health Service (NHS) had been subjected to some type of ransomware attack.

The TrapX Report (2018) describes Medical Device Hijack, or Medjack, as an attack where malware is injected into unsecured medical devices to traverse the hospital network. Typically, the attack begins with reconnaissance to find a suitable vector. A common method involves injecting an executable by plugging a USB thumb drive into a device within the hospital network, thereby establishing a foothold (TrapX Research Labs, 2018).

Hospital security systems can be compromised through infected medical devices, including ventilators, infusion pumps, and MRI machines, among other therapeutic and diagnostic tools (TrapX Research Labs, 2018). Workers from Quality Software Services Inc. (QSSI) managed to connect unauthorised USB devices to USB ports in 2013, posing a threat to approximately 6 million dollars of Medicare beneficiaries (Bowman, 2013; Daly, 2013).

Given the concerns, the NIS2 directive and GDPR have been established to mandate a uniform level of cybersecurity across the EU and the European Economic Area (EEA). Against this backdrop, this project aims to tackle the issue of GDPR and NIS2 regulatory concerns arising from USB injection threats in the healthcare sector.

This study provides comprehensive solutions to mitigate the risks outlined, which fall into two main categories. Firstly, it's crucial to prevent unauthorised physical access to the machine by a malicious actor. Secondly, network and data must safeguard against the possibility of a threat actor successfully introducing a USB drive, despite the security precautions in place. The study centres on the risks posed by malicious executable code within the healthcare sector. It specifically addresses the scenario in which an unauthorised USB thumb drive is inserted into a hospital's Point of Care Testing (POCT) machine, creating the potential for malware to spread throughout the hospital's network and servers. POCT machines are diagnostic devices that perform medical tests at or near the patient's care site and provide fast results. These machines are often employed in hospitals, clinics, and even at home to quickly diagnose e.g. infections, metabolic disorders, and cardiac events (F. Hoffmann-La Roche Ltd, 2024; Randox Laboratories Ltd., 2024; Sohn et al., 2016). This study aims to identify and comprehend the vulnerabilities associated with USB devices within the framework of regulatory standards. The goal is to assist organisations in achieving compliance with the GDPR and the NIS2, thereby enhancing their resilience against cyber threats.

The research question is: What vulnerabilities do USB devices introduce into healthcare systems, and how do they conflict with GDPR and NIS2 requirements?

The paper is organised into five sections: Section 2 offers a Literature review; Section 3 outlines the study's methodology, encompassing the approach, case environment, research process, and materials used; Section 4 details the results; and Section 5 discusses the findings, concluding with the study's implications.

2. Literature Review

Cybersecurity incidents have become a growing problem for the healthcare industry since the widespread introduction of technology into healthcare systems (Kruse et al., 2017). In recent years, the number of attacks has increased rapidly, making healthcare one of the most targeted sectors globally (Newaz et al., 2021). These attacks threaten not only the data and finances of medical organisations but also disrupt hospital operations and endanger patient health and well-being. Traditional security measures are insufficient to protect the healthcare IT environment due to its complexity and the heterogeneity of medical devices. (Ghourabi, 2022).

Universal Serial Bus (USB) is the most commonly used standard for peripheral communications in 5G generation computer systems. USB is also used for charging devices. However, USB is susceptible to various security threats. (Singh et al., 2022). So, it is crucial to use physical barriers or software solutions such as disabling USB ports and ensuring employees understand the risks (Nissim et al., 2017).

Recent case studies have underscored the grave risk that USB malware presents to healthcare systems. In a prominent incident, a healthcare facility was compromised by an advanced cyberattack initiated through a contaminated USB drive connected to hospital computers (Check Point Research, 2023). The malware, concealed within files that appeared harmless, rapidly propagated across the network, encrypting vital patient information, and making crucial medical services unavailable.

In another case, a hospital's IT infrastructure was compromised by USB malware, introduced by a malevolent individual masquerading as an authorised visitor. The intruder cunningly deployed a USB device in critical

locations, taking advantage of lapses in the hospital's security protocols. The violation caused considerable interference with patient services, as healthcare professionals faced difficulties retrieving essential patient information and providing prompt care (Security Week News, 2023).

Moreover, a study by cybersecurity experts has uncovered numerous instances of USB malware compromising healthcare systems globally. These incidents highlight the critical need for enhanced cybersecurity protocols within healthcare organisations to avert future intrusions and safeguard patient data confidentiality. The surge in USB malware attacks within healthcare environments represents a significant danger to patient safety and data protection. Consequently, healthcare institutions must elevate cybersecurity as a priority and establish comprehensive strategies to diminish the risks associated with USB devices (Thamer & Alubady, 2021).

Many healthcare systems depend on outdated operating systems, which makes them susceptible to exploitation due to unpatched vulnerabilities. If USB devices are connected, attackers can exploit these vulnerabilities to gain unauthorised access (Daly, 2013). Inadequate credential management leads to insecure practices, such as the use of hardcoded credentials or weak passwords, creating security gaps. Attackers can use USB access to exploit these credentials and breach healthcare systems (Department of Homeland Security, 2012). Additionally, healthcare systems are at risk of injection attacks if they lack proper input verification and sanitisation. Attackers can use USB devices to perform malicious actions like SQL injection, compromising the integrity of the system (Mejía-Granda et al., 2024).

USB devices can serve as a conduit for the spread of malware. For example, juice jacking is a popular and spreading cyberattack that allows intruders to access the system through the network and steal potential data from the system (Singh et al., 2022). When a healthcare system is compromised through a USB connection, it endangers patient data security, business operations, and patient safety (Mejía-Granda et al., 2024). The insufficient security infrastructure for IoT devices is also problematic for the healthcare industry. The incorporation of IoT devices into healthcare systems increases the potential for cyber-attacks. It is crucial to secure communication channels, implement robust software practices, and ensure continuous security measures to safeguard medical devices from cyber threats (Mejía-Granda et al., 2024).

To address these vulnerabilities, a multi-layered strategy is necessary, encompassing reconfiguration, robust certificate management, stringent input authentication, malware protection, and a thorough IoT security plan (Mejía-Granda et al., 2024). Healthcare organisations can mitigate USB malware threats by consistently updating and patching systems, implementing strong credential management with complex passwords and multi-factor authentication, and conducting proper input validation to avert injection attacks. Utilising an advanced antivirus tool and securing all IoT devices with robust communication and software practices are also vital in preventing these malicious activities.

Healthcare organisations should enforce stringent security measures such as keycards, biometric scanners, and visitor escorts to prevent unauthorised physical access. Additionally, they need to limit the use of personal USB devices, as these are a primary vector for malware transmission in the healthcare sector. Lastly, the crucial step is to educate staff on security protocols and install surveillance cameras and monitoring systems in sensitive areas to bolster overall security.

3. Method

This study examines hospital cybersecurity and compliance with GDPR and NIS2 requirements through a specific scenario “USB Infection of a point-of-care testing machine” because it has been identified as a clear threat vector in the Dynamic Resilience Assessment Method including a combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors (DYNAMO) project. The DYNAMO project is designed to investigate how distractions affect the critical sectors of healthcare, energy, and maritime transport. The DYNAMO project advocates for an integrated approach to improve cyber situational awareness for critical sectors (DYNAMO project, 2024). Recent research on USB malware threats in healthcare emphasises the continuous and changing security risks associated with USB peripherals. (Jofre et al., 2021) and (Ticu, 2019) have pointed out the dangers USB devices pose to health systems. (Ticu, 2019) categorised these dangers into various malicious activities, including keystroke injection and data extraction. The threats to sensitive health information are especially perilous due to the potential for significant harm if compromised. Despite long-standing recognition of these risks, the literature indicates that the threat landscape is still evolving, with new methods and tools being developed to exploit vulnerabilities. These findings underscore the need for ongoing emphasis on robust cybersecurity practices and heightened awareness among healthcare professionals to reduce the risks associated with USB malware. (Jofre et al., 2021; Ticu, 2019).

Healthcare cybersecurity data collection focuses primarily on qualitative data that provides valuable insight into the complex cyber threat environment, the effectiveness of security measures, and practical approaches to mitigating risks. Furthermore, enriching primary insights with secondary data from various sources, including academic papers, incident reports, policy documents, and case studies, helped to frame our analysis. This secondary data is crucial for creating a thorough framework to evaluate the risks that physical malware delivery poses to healthcare organisations.

This study outlines the necessary steps to ensure compliance with GDPR and NIS2 thereby enhancing resilience against cyber threats.

4. Case Study – USB Infection of a Point-Of-Care Testing Machine

Cyber risk management is widely recognised as a critical issue for many organisations. The healthcare sector, particularly hospitals, is increasingly threatened by cybersecurity and privacy breaches (World Economic Forum, 2024). Unfortunately, this sector has often failed to prioritise the safety of key stakeholders, including healthcare workers and patients. Consequently, hospitals are compelled to invest substantial resources and capital to fortify their IT systems (Jofre et al., 2021). We explore the necessary steps for health organisations to achieve GDPR and NIS2 compliance, thereby addressing the risk of USB injection. The healthcare industry must act swiftly and decisively to mitigate this escalating threat and safeguard the well-being and security of all stakeholders.

In the current technology-centric era, hospitals represent intricate entities laden with substantial technological integration, internal political dynamics, and regulatory demands. Consequently, the shift towards more secure and robust digital infrastructures poses considerable challenges for healthcare institutions. Nonetheless, to realise their objectives, these organisations must comprehend and incorporate the capabilities, motivations, strategies, and obstacles inherent in related domains, including cybersecurity and data privacy.

4.1 Scenario Overview

The case study scenario is an attack on the hospital's Laboratory Information System (LIS), through which the attacker can disrupt hospital operations. The attacker can also target the Hospital Information System (HIS), which grants access to the hospital environment allowing them to shut down hospital systems and force employees to revert to manual operations, which are very slow and completely prone to errors. All this access occurs if an unidentified user inserts some software via a USB key into the point-of-care testing (POCT) machine.

4.2 Managing the Physical Threat

Physical security of POCT devices requires training and awareness among staff. When not in use, it is recommended to store these machines in a locked cabinet or container. Hospital staff should be informed about the risks of unattended or improper handling of these devices. It is advisable to use USB port locks if USB devices are unnecessary for the machine's operation. It is also suggested to monitor and keep track of people's access to areas near POCT machines. Keeping these machines out of public spaces like lobbies, waiting rooms, hallways, or cafeterias is advisable. Regular inspections are necessary to verify adherence to security protocols and the effectiveness of staff training. It's important to report any suspicious activities immediately.

4.3 Managing the Case of USB Injection

The previous section covered how to prevent threat actors from using a USB thumb drive to compromise a POCT machine. This section will detail the necessary steps to mitigate the harm caused by malicious software, dividing the content into preventive measures and an incident response plan. Preventive measures encompass network security, user training, policies, and endpoint protection. Network security involves network segmentation, along with the deployment of firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). Isolating POCT machines from the main hospital network can reduce the risk of malware spreading to the hospital's servers. This isolation necessitates a dedicated subnet or Virtual Local Area Network (VLAN) specifically for POCT machines.

Preventive measures should encompass staff training to enhance awareness and enforce stringent policies for USB drive usage. Additionally, endpoint security solutions like antivirus and anti-malware software are essential and must be regularly updated. This software ought to be set up to automatically scan USB devices upon connection to the system, and only authorised devices should be permitted to connect.

Maintaining up-to-date antivirus and antimalware solutions is crucial. POCT machines typically operate on one of three main operating systems: Windows Embedded, various Linux-based systems, or Android. These platforms are chosen for their stability, security features, and ability to support specialised functions critical for

medical diagnostics and data handling. Companies such as Siemens Healthineers, Abbott Laboratories, and Roche frequently employ proprietary systems tailored for their equipment, guaranteeing compatibility with their software and hardware components. It is essential to choose endpoint protection software that is compatible with the specific platform in use.

An incident response plan should include continuous system monitoring and the capability for immediate isolation if malware is detected. An incident response team should be prepared for scenarios like USB injection. Before removing the malware, it is crucial to isolate the issue and secure any sensitive patient data on the POCT machine. While POCT machines should not store patient data, any critical data that is otherwise irretrievable must be extracted and preserved. The appropriate action is to reset the infected POCT machine before it is used again in production environments.

An essential component of the incident response plan is communication, both internal and external. Hospital staff must be informed about the incident, and, if necessary, external stakeholders should be alerted. These external parties might include health officials. While some safety measures, including communication protocols, may not be unique to USB injection incidents, they must be implemented regardless. They are referenced here to emphasise their relevance to even highly specific scenarios.

4.4 Recovery Procedures to Ensure Business Continuity

This section outlines the recovery procedures following a catastrophic security incident. While these recovery procedures are not exclusive to USB injection incidents, they also apply to the topic. In the event of a security breach due to USB injection, planning for data backup, restoration, and system recovery is essential. Additionally, for business continuity and ongoing improvement, conducting a post-incident review that includes root cause analysis and devising an improvement plan is essential. Backing up the data from POCT machines is not required once data has been transferred to the hospital's servers, which should be done promptly. Nevertheless, it is crucial to have plans for data backup and restoration for these servers. Should a security incident hinder data transfer from the POCT machine to the servers, a restoration plan is essential. Restoring the POCT machine's system necessitates a complete wipe. Since data storage on POCT machines is not advisable, only system restoration is necessary. To facilitate this, updated system images must be accessible.

5. The Impact of GDPR and NIS2 on Hospital’s Cybersecurity Measures

It is crucial to determine the format of a Data Protection Impact Assessment (DPIA) and what data would be included in the Critical Threat Intelligence (CTI) exchange. With the introduction of GDPR, the management of personal data will be improved in addition to compliance with laws. NIS2 does not specify that every hospital must have an Intrusion Prevention System (IPS) or Intrusion Detecting System (IDS) in their network but sets broader requirements that could be partially met by installing such systems.

5.1 GDPR Landscape

Projects such as DYNAMO are recommended to prepare a DPIA due to the risk of GDPR breaches involving others’ data. This assessment should outline the risks to individuals’ rights and freedoms, justify the need for data processing and its intended purpose, and include mechanisms to ensure personal data protection considering legitimate interests. It is important to note that there is no set format for such an assessment—while recommended templates are available, this area can be somewhat complex for those implementing the legislation. One primary advantage of implementing GDPR controls is that, while the main objective is achieving legal compliance, the project will also enhance control over patients’ personal information, providing an ethical benefit.

To ensure compliance during CTI exchanges, DYNAMO should anonymise identifiable data such as personal and health information. This involves closely monitoring outgoing data and effectively applying anonymisation techniques, which will require proper tools to ensure successful anonymisation.

In the scenario described the attacker accesses or uses the laboratory information system and the hospital information system. In this case, it can be assumed that the following data containing personal information may be used:

- Technical data – e.g., IP addresses, hardware specifications, network architecture
- Health-related data – e.g., test results, details of medical conditions
- Personal data – e.g., names and surnames of patients and hospital workers, insurance information.

5.2 NIS2 Landscape

NIS2 overlaps significantly with cyber threat intelligence (CTI) sharing. Article 7 guides the national cybersecurity strategy, which includes:

- Identifying measures to ensure preparedness for, responsiveness to, and recovery from incidents, including public and private sector cooperation.
- Managing vulnerabilities, including promoting and facilitating coordinated vulnerability disclosure under Article 12.
- Including relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between entities under Union law.

Article 12 sets measures for coordinated vulnerability disclosure, with national-level CSIRTs (Computer Security Incident Response Teams) responsible for coordinating measures such as assisting legal entities in reporting vulnerabilities. Chapter III of NIS2 is dedicated to cooperation at the union and international levels.

Article 21 outlines cybersecurity risk management measures aimed at protecting network and information systems and their physical environments from incidents. Article 20 requires Member States to ensure that all affected entities approve the cybersecurity risk management measures in Article 21. For CTI sharing, the main measures in Article 21 include:

- Risk analysis and information system security policies
- Incident handling
- Business continuity
- Supply chain security
- Security in network and information systems acquisition, including vulnerability handling and disclosure
- Policies and procedures to assess the effectiveness of cybersecurity risk management measures
- Basic cyber hygiene practices and cybersecurity training
- Policies and procedures regarding the use of cryptography and encryption
- Use of multi-factor authentication and secured communication systems within the entity, where appropriate

Article 23 details reporting obligations. Member States must ensure that significant incidents, which cause or can cause severe operational disruption or financial loss or affect other natural or legal persons by causing considerable material or non-material damage, are reported without undue delay to CSIRT or the competent authority to determine any cross-border impact. Article 23 specifies two timeframes: 24 and 72 hours. An early warning must be provided within 24 hours of discovering a significant incident, indicating whether it is suspected to be caused by unlawful or malicious acts or could have a cross-border impact. Within 72 hours, an initial assessment of the incident's severity and impact, including indicators of compromise if available, must be provided.

Article 24 allows Member States to set requirements for using ICT services and processes certified under European cybersecurity certification schemes. CTI systems should be developed to be accredited and certified if required. NIS2 introduces administrative fines, with Articles 21 and 23 being enforceable and subject to penalties for non-compliance.

Examining the scenario in the context of NIS2 compliance, it can be concluded that NIS2 specifically covers the scenario in Articles 7, 12, 21, and 23. These articles pertain to a broad set of requirements for management, training, and technical tools for security in general. NIS2 does not specify that every hospital must have an Intrusion Prevention System (IPS) or Intrusion Detecting System (IDS) in their network but sets broader requirements that could be partially met by installing such systems. The technical details are left to the organisation to decide to achieve compliance with the NIS2 directive. The examined scenarios are subject to the mandatory incident reporting regime established by NIS2, requiring actions to be taken towards the national CSIRT within 24 hours of becoming aware of the incident, with sanctions for non-compliance. The extent of information sharing must be assessed by the notifier to meet NIS2 requirements while complying with other regulations such as GDPR.

6. Discussion and Conclusions

The healthcare sector faces significant cybersecurity challenges, particularly with the threat of USB injection attacks. These attacks can disrupt critical healthcare services and compromise sensitive patient data. The GDPR and the NIS2 Directive impose stringent requirements to protect against such threats. Healthcare organisations must implement robust security measures and promptly report data breaches as part of GDPR's mandate to protect personal data. Under NIS2, healthcare entities are tasked with managing cyber risks, securing supply chains, and ensuring the continuity of essential services, building on the original NIS Directive. Compliance with these regulations is crucial, especially when USB injection attacks result in unauthorised access to patient information. Healthcare organisations need to implement comprehensive cybersecurity strategies, including frequent employee training, updated technology, and incident response plans, to avoid these risks and comply with GDPR and NIS2 requirements.

Organisations are required to restrict data collection to clearly defined purposes, guarantee data accuracy, set limits on retention periods, and be accountable for compliance while safeguarding the integrity and confidentiality of the data. They must also obtain explicit consent from individuals for data processing and promptly report any data breaches. (Wolford, 2018). In addition, plans for addressing security incidents and managing operations during such events are compulsory. Consideration of cybersecurity training and supply chain security is necessary, and ultimately, policies to assess the effectiveness of these measures are required. The NIS2 Directive imposes additional requirements beyond those of the GDPR. While this may increase the costs of services in the health sector, adherence will enhance resilience against cyber threats.

The storage of patient data on the hospital's servers necessitates a focus on thwarting unauthorised physical access to POCT machines. Additionally, if a USB device is used, it is crucial to secure the POCT machines themselves to prevent malware from infiltrating the network. Although POCT terminals represent just one device type within hospital settings, the limited scope of our project is far from trivial. Given the current threat landscape, where nation-scale threat actors are more active, it is imperative to seal every potential entry point.

Cybersecurity is increasingly vital in healthcare as the adoption of digital technologies grows, and the threat of cyber-attacks rises in tandem. This study highlights the importance of robust strategies to safeguard physical and digital infrastructures, ensuring the security of patient data and healthcare services. By implementing strong security measures, protocols, and response plans, healthcare providers can fortify themselves against the pervasive risks of cyber-attacks. The objective of this study was to demonstrate the critical importance of aligning cybersecurity practices with the rigorous regulatory standards established by the GDPR and NIS2. Achieving compliance through technical improvements and procedural changes is essential for safeguarding the privacy and integrity of patient data within systems. Adherence to these regulations is obligatory and advantageous, as a secure information environment enhances patient confidence in the healthcare system.

This approach emphasises the importance of managing physical threats, which includes limiting access to POCT machines and addressing the risk of a malicious USB drive being inserted into one. It involves implementing preventive controls and establishing an incident response plan. Additionally, the necessary measures for disaster recovery are detailed. Achieving a fully safe and compliant healthcare environment is fraught with challenges. Numerous hurdles exist, such as implementing consistent safety measures across disparate systems and integrating new security technologies into existing infrastructures. Moreover, navigating the intricate maze of regulatory requirements adds an additional layer of complexity to this critical endeavour.

In summary, despite the multitude of challenges, the suggested strategies offer a clear path forward. Organisations can strengthen their defences against emerging cyber threats by fostering a culture of continuous improvement and compliance, investing in the modernisation of outdated systems, and treating cybersecurity as a critical component of healthcare service provision. This proactive approach goes beyond mere compliance or safeguarding the institution—it is about preserving the essence of healthcare: ensuring the safety and well-being of patients.

Subsequent research should refine the methodologies used in this study, and the approaches outlined in Chapter 4 could be improved with clearer definitions.

Acknowledgements

This study has received funding from the European Union project DYNAMO, the European Union’s Horizon 2020 research and innovation programme under the grant agreement no. 101069601 and The Cybersecurity in Everyday Work in the Social and Healthcare Sector (KyberSoTe) project funded by the National Emergency

Supply Agency. The views expressed are those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

References

Bowman, D. (2013, June 19). *Poor USB security puts info for 6 million Medicare beneficiaries at risk*. https://www.fiercehealthcare.com/it/poor-usb-security-puts-info-for-6-million-medicare-beneficiaries-at-risk

Check Point Research. (2023, June 22). *Beyond the Horizon: Traveling the World on Camaro Dragon's USB Flash Drives*. Check Point Research. https://research.checkpoint.com/2023/beyond-the-horizon-traveling-the-world-on-camaro-dragons-usb-flash-drives/

Cybersecurity & Infrastructure Security Agency. (2024, November 19). *More than a Password*. Cybersecurity Best Practices. https://www.cisa.gov/MFA

Daly, K. L. (2013). *Quality Software Services had not implemented Universal Serial Bus Device and ports controls* (No. A-04-12-05045; p. 16). Department of Health and Human Services. https://oig.hhs.gov/oas/reports/region4/41205045.pdf

Department of Homeland Security. (2012). *Attack Surface: Healthcare and Public Health Sector* (No. 201205040900; p. 10). National Cybersecurity and Communications Integration Center. https://info.publicintelligence.net/NCCIC-MedicalDevices.pdf

DYNAMO project. (2024, January 9). *DYNAMO Mission and Objectives*. https://horizon-dynamo.eu/about/

European Parliament and of the Council. (2024, November 8). *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) | Shaping Europe's digital future*. European Parliament. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

European Parliament and the Council. (2016, April 27). *General Data Protection Regulation (GDPR)*. European Parliament. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504

F. Hoffmann-La Roche Ltd. (2024, November 19). *Point of Care testing solutions*. Diagnostics. https://diagnostics.roche.com/global/en/products/product-category/lab-type/point-of-care-testing-poct.html

Ghourabi, A. (2022). A Security Model Based on LightGBM and Transformer to Protect Healthcare Systems From Cyberattacks. *IEEE Access*, *10*, 48890–48903. IEEE Access. https://doi.org/10.1109/ACCESS.2022.3172432

Jofre, M., Navarro-Llobet, D., Agulló, R., Puig, J., Gonzalez-Granadillo, G., Mora Zamorano, J., & Romeu, R. (2021). Cybersecurity and Privacy Risk Assessment of Point-of-Care Systems in Healthcare—A Use Case Approach. *Applied Sciences*, *11*(15), Article 15. https://doi.org/10.3390/app11156699

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care: Official Journal of the European Society for Engineering and Medicine*, *25*(1), 1–10. https://doi.org/10.3233/THC-161263

Mansfield-Devine, S. (2016). Ransomware: Taking businesses hostage. *Network Security*, *2016*(10), 8–17. https://doi.org/10.1016/S1353-4858(16)30096-4

Mejía-Granda, C. M., Fernández-Alemán, J. L., Carrillo-de-Gea, J. M., & García-Berná, J. A. (2024). Security vulnerabilities in healthcare: An analysis of medical devices and software. *Medical & Biological Engineering & Computing*, *62*(1), 257–273. https://doi.org/10.1007/s11517-023-02912-0

Newaz, A. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2021). A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks and Defenses. *ACM Transactions on Computing for Healthcare*, *2*(3), 1–44. https://doi.org/10.1145/3453176

Nissim, N., Yahalom, R., & Elovici, Y. (2017). USB-based attacks. *Computers & Security*, *70*, 675–688. https://doi.org/10.1016/j.cose.2017.08.002

Randox Laboratories Ltd. (2024). Point of Care Testing (POCT) Explained. *Randox Laboratories*. https://www.randox.com/poct-explained/

Security Week News. (2023, June 30). *In Other News: Hospital Infected via USB Drive, EU Cybersecurity Rules, Free Security Tools*. SecurityWeek. https://www.securityweek.com/in-other-news-hospital-infected-via-usb-drive-eu-cybersecurity-rules-free-security-tools/

Singh, D., Biswal, A. K., Samanta, D., Singh, D., & Lee, H.-N. (2022). Juice jacking: Security issues and improvements in USB technology. *Sustainability*, *14*(2), 939. https://doi.org/10.3390/su14020939

Sohn, A. J., Hickner, J. M., & Alem, F. (2016). Use of Point-of-Care Tests (POCTs) by US Primary Care Physicians. *The Journal of the American Board of Family Medicine*, *29*(3), 371–376. https://doi.org/10.3122/jabfm.2016.03.150249

Thamer, N., & Alubady, R. (2021). *A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research*. 210–216. https://doi.org/10.1109/BICITS51482.2021.9509877

Ticu, M. (2019). Raising awareness of cyber security concerns regarding the use of USB peripherals. *Romanian Cyber Security Journal*, *1*(1), 87–92.

TrapX Research Labs. (2018). *Medical Device Hijacking* (Investigative Report No. MEDJACK.4; p. 29). TrapX Security, Inc. https://www.trustdimension.com/wp-content/uploads/2015/02/MedJack.4-ilovepdf-compressed.pdf

Wolford, B. (2018, November 7). *What is GDPR, the EU's new data protection law?* GDPR.Eu. https://gdpr.eu/what-is-gdpr/

World Economic Forum. (2024, February 1). *Why the healthcare industry must prioritize cyber resilience*. World Economic Forum. https://www.weforum.org/agenda/2024/02/healthcare-pays-the-highest-price-of-any-sector-for-cyberattacks-that-why-cyber-resilience-is-key/