A Governance Model for Cyber Threat Information Sharing in the Healthcare Sector

Jyri Rajamäki[1][1] and Ilkka Tikanmäki[1,2][2]
[1]Business, Data Processing and Service Sector Unit, Laurea University of Applied Sciences, Espoo, Finland
[2]National Defence University, Helsinki, Finland

jyri.rajamaki@laurea.fi
Ilkka.tikanmaki@laurea.fi

Abstract: Cyber Threat Information (CTI) sharing is a vital component of cybersecurity in the healthcare sector, where protecting sensitive patient data and the continuity of critical services are paramount. It's implementing faces socio-technical complexity and strict EU requirements, including the General Data Protection Regulation (GDPR), the Network and Information Security Directive 2 (NIS2), the Cyber Resilience Act (CRA), and the AI Act. This paper applies the Design Science Research (DSR) methodology to develop a governance model that enables secure, compliant, and context-aware CTI sharing. The model integrates systems theory, socio-technical principles, information systems governance, and cyber resilience. It is informed by empirical studies and practical insights from SOC/CERT frameworks. It leverages the DYNAMO platform and tools such as Early Warning System (EWS), open-source software solution MISP, and Data Anonymisation Tool (DAT), to support structured, interoperable, and regulation-compliant threat intelligence exchange. A phased implementation strategy is outlined, beginning with pilot testing in hospitals, then regional integration with CERTs, culminating in national deployment. Evaluation is conducted using realistic assessment and case analysis, with metrics guiding iterative refinement. The model addresses the research question: *How can a governance model for cyber threat information sharing be designed for the healthcare sector under EU regulatory constraints?* This work contributes a scalable, adaptable governance framework that enhances cyber resilience and fosters trust-based collaboration across healthcare ecosystems.

Keywords: Cyber threat intelligence, Healthcare cybersecurity, ECHO early warning system, Interoperability, Design science

1. Introduction

Cybersecurity in healthcare is a growing concern due to the sensitivity of patient data and the critical nature of healthcare services. Recent attacks have demonstrated the vulnerability of hospital systems and the lack of coordinated response mechanisms. The healthcare sector faces increasing cybersecurity threats, ranging from ransomware attacks to data breaches involving sensitive patient information. Sharing cyber threat intelligence (CTI) among stakeholders, such as hospitals, national CERTs, and EU-level agencies, is essential for proactive defence. However, CTI in healthcare is constrained by legal, technical, and organisational factors. Existing CTI sharing systems are either fragmented or nonexistent. The European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO) project introduced the ECHO Early Warning System (E-EWS) to facilitate cross-sectoral threat sharing, while the Malware Information Sharing Platform (MISP) provides a structured taxonomy for external data exchange. (Chalkias et al., 2023)

The Early Warning System plays a pivotal role in the CTI workflow by serving as a central platform for collecting, analysing, and disseminating threat information. Within the Dynamic Resilience Assessment Method, including a combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors (DYNAMO) framework (DYNAMO project, 2024b), E-EWS integrates both internal and external data sources to generate actionable intelligence (Lahdenperä et al., 2022). Internal sources include logs from the Intrusion Detection System/ Intrusion Prevention System (IDS/IPS), honeypots, and organisational infrastructure, while external sources span Surface Web, Deep Web, and Dark Web content.

Gathering threat data, the system employs multiple crawling techniques. Simple Crawling for indexing URLs, Focused Crawling for CTI-relevant content based on confidence thresholds, and Evasive Crawling to mimic human browsing behaviour and avoid bot detection. These methods ensure comprehensive coverage of threat vectors and indicators. Once data is collected, it undergoes correlation analysis using rule-based and machine learning techniques. The MISP correlation engine identifies relationships between attributes such as hash values and IP addresses. Advanced methods apply text similarity algorithms to detect related threats across different sources. This enables the mapping of tactics, techniques, and procedures (TTPs) used by threat actors (Sun et

[1]https://orcid.org/0000–0003–4798–2462

[2]https://orcid.org/0000- 0001-8950-5221

al., 2023). To ensure privacy and compliance, the Data Anonymisation Tool (DAT) is used to sanitise CTI reports before sharing. It applies Natural Language Processing (NLP) to extract sensitive entities and anonymise them according to predefined policies, protecting identifiers, quasi-identifiers, and confidential attributes (DYNAMO project, 2024a).

Structured sharing of CTI is facilitated through the MISP and Structured Threat Information Expression (STIX) 2.1 format, enabling interoperability and secure exchange of threat intelligence across organisations. Fine-grained access control is enforced using Attribute-Based Encryption (ABE), ensuring that only authorised entities can decrypt and access shared data. This integrated approach enhances situational awareness, supports proactive defence strategies, and strengthens cyber resilience in the healthcare sector. (DYNAMO project, 2024a)

This paper addresses the research problem: How can a governance model for cyber threat information sharing be designed for the healthcare sector under EU regulatory constraints?

The rest of this article is structured as follows: Section 2 presents the Design Science Research methodology; Section 3 describes the healthcare cybersecurity environment and regulatory context. Section 4 presents the knowledge base underlying the governance model. Section 5 provides a detailed explanation of the governance model design. Section 6 focuses on the evaluation and implementation strategy. Finally, Section 7 summarises the article and provides future research directions.

2. Methodology: Design Science Research Framework

The study follows Hevner's Design Science Research (DSR) framework, as shown in Fig. 1 (Hevner, 2007). It consists of three interrelated cycles: relevance, rigour and design. The practical problem is defined in the relevance cycle; the need for a governance model enables a secure and legally compliant Clinical Trials Information System (CTIS) in healthcare. In the rigour cycle, the design is grounded in existing knowledge bases, including systems theory, socio-technical theory, information systems governance models, and risk management theories. Iterative development and evaluation of the governance model is done during the design cycle using design models, evaluation frameworks (e.g. realistic assessment, case analysis), and modeling methods like Business Process Model and Notation (BPMN) and Unified Modeling Language (UML).

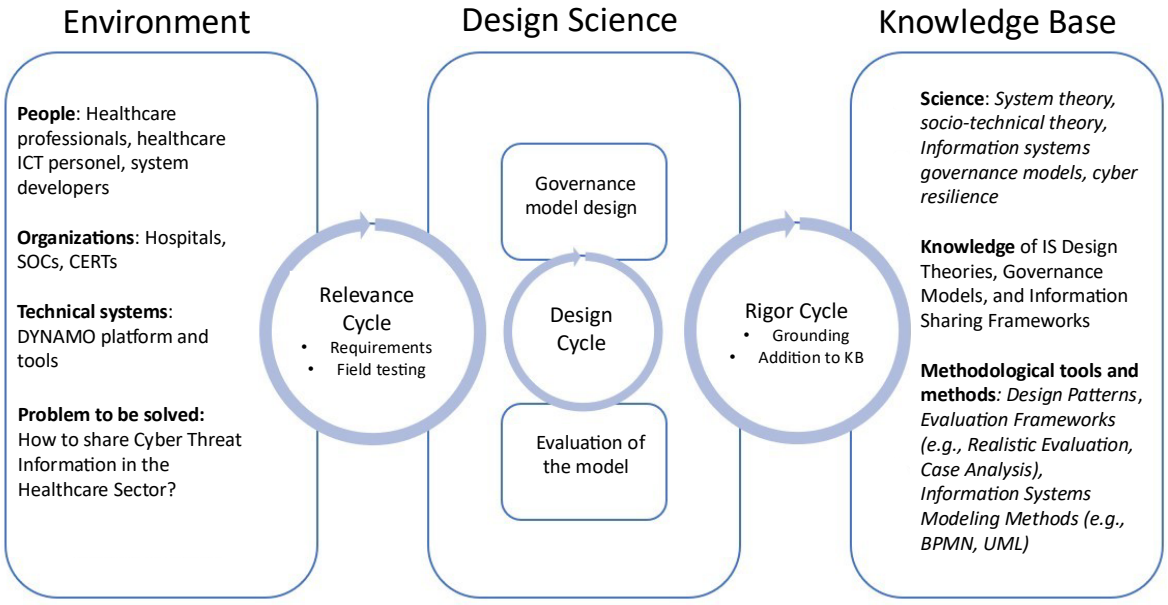

Figure 1: Applied Design Science Research Framework. Adapted from (Hevner, 2007)

Sources include the World Health Organization (WHO), the European Union Agency for Cybersecurity (ENISA), EU policy documents, and peer-reviewed literature. A model-based analysis evaluates the applicability of ECHO's governance model and MISP integration, focusing on role-based access control, interoperability, and legal compliance.

3. Environment

3.1 People

Healthcare professionals, ICT personnel, and system developers constitute the core stakeholder groups in this research. Each of them is contributing essential expertise to the design and implementation of cyber threat information sharing systems in the healthcare sector. Healthcare professionals provide domain-specific knowledge and clinical insights that are critical for aligning technological solutions with real-world medical workflows and patient care requirements. Their involvement ensures that the governance model and supporting systems are not only technically sound but also practically applicable and user-centred.

Healthcare ICT personnel serve as intermediaries between clinical operations and technological infrastructure. Their dual expertise in healthcare processes and information systems enables them to facilitate the integration, configuration, and maintenance of cybersecurity tools and platforms within healthcare organisations. They play a pivotal role in operationalising threat intelligence workflows and ensuring compliance with institutional and regulatory standards.

System developers contribute the technical foundation necessary for building secure, scalable, and interoperable systems. Their collaboration with healthcare professionals and ICT personnel is essential for translating functional requirements into robust software architectures. Developers are responsible for implementing features such as data anonymisation, threat correlation engines, and secure sharing protocols, all of which are central to the proposed governance model. Together, these groups form a multidisciplinary ecosystem that supports the development of resilient and regulation-compliant cyber threat information sharing frameworks tailored to the healthcare domain.

3.2 The DYNAMO Platform and Toolset

The DYNAMO platform is an AI-driven framework developed under the Horizon Europe programme to enhance cyber resilience across critical sectors, including healthcare, energy, and maritime domains. Its primary objective is to support decision-making in cyber threat mitigation and business continuity management (BCM) through integrated threat intelligence workflows. In the healthcare context, DYNAMO facilitates secure, regulation-compliant, and context-aware cyber threat information (CTI) sharing among stakeholders.

At the core of DYNAMO is the Early Warning System (EWS), which serves as a central hub for collecting, analysing, and disseminating threat intelligence. EWS aggregates data from both internal and external sources. Internal sources include intrusion detection and prevention system (IDS/IPS) logs, honeypots, and organisational infrastructure telemetry.

External sources span the Surface Web, Deep Web, and Dark Web, enabling comprehensive threat landscape coverage. EWS gathers threat intelligence through a multi-layered indexing architecture. Simple Crawling indexes URLs for general threat indicators, Focused Crawling targets CTI-relevant content based on trust thresholds, and Evasive Crawling mimics human browsing behaviour to bypass bot detection mechanisms.

Once data is acquired, it undergoes correlation analysis using both rule-based logic and machine learning algorithms. The platform leverages the MISP correlation engine to identify relationships between threat attributes such as hash values, IP addresses, and domain names. Advanced text similarity techniques are applied to detect related threats across heterogeneous sources, enabling the mapping of tactics, techniques, and procedures (TTPs) employed by threat actors.

To ensure compliance with privacy regulations such as GDPR, the Data Anonymisation Tool (DAT) is integrated into the workflow. DAT utilises Natural Language Processing (NLP) to identify and anonymise sensitive entities in CTI reports, including identifiers, quasi-identifiers, and confidential attributes, based on predefined policy rules. (DYNAMO project, 2024a)

Structured sharing of CTI is facilitated through the Malware Information Sharing Platform (MISP) and the STIX 2.1 format, ensuring interoperability and semantic consistency across organisations. Fine-grained access control is enforced using Attribute-Based Encryption (ABE), which guarantees that only authorised entities can decrypt and access shared intelligence.

This integrated toolset enhances situational awareness, supports proactive defence strategies, and strengthens cyber resilience in healthcare environments. It also aligns with EU regulatory frameworks, making it a viable foundation for governance models aimed at secure and compliant CTIS implementation. (DYNAMO project, 2024a)

3.3 Regulatory Context and its Impact on CTIS

EU regulations are significantly shaping the design space for CTIS, with GDPR setting strict rules for sharing personal data, requiring anonymisation and legal justification. NIS2 requires breach reporting and cooperation between key actors, including healthcare providers. The CRA introduces cybersecurity requirements for connected devices, which are relevant for medical IoT systems.

The AI Act regulates the use of AI in sensitive sectors, such as healthcare, and impacts automated threat detection and response. These provisions create both constraints and opportunities for governance design, as highlighted in recent studies and policy documents.

3.4 Compliance within the EU Cybersecurity Legal Framework

The EU cybersecurity regulatory landscape has evolved significantly in recent years, particularly with the introduction of the NIS2 Directive, the Cyber Resilience Act (CRA), and the Corporate Sustainability Reporting Directive (CSRD). This article examines how external Security Operations Centre (SOC) services can support organisations in demonstrating compliance with these regulations. SOC services can substantially enhance an organisation's ability to meet regulatory requirements, produce audit-ready documentation, and report cybersecurity measures to stakeholders.

EU cybersecurity legislation requires organisations to implement technical, organisational, and operational measures to manage cyber risks. Demonstrating compliance is a critical aspect of regulatory implementation, and external SOC services can play a key role in this process. SOCs provide continuous threat monitoring, incident response, log management, and reporting—core elements for evidencing compliance.

3.4.1 NIS2 directive and SOCsServices

The NIS2 Directive (EU 2022/2555) mandates risk-based cybersecurity measures (Article 21) and requires management involvement in cybersecurity governance (Article 20). SOCs can support organisations by:

- Providing real-time threat monitoring and response (Article 21)
- Assisting with incident notification obligations (Article 23): 24h early warning, 72h incident report, 1-month final report
- Supporting executive training and accountability (Article 20)

The directive aims to harmonise cybersecurity practices across the EU and improve the quality and comparability of reporting (Vandezande, 2023).

3.4.2 Cyber resilience act and technical support from SOCs

The CRA (EU Proposal 2022/454) sets requirements for digital products, especially IoT devices (European Commission, 2022). SOCs can assist manufacturers and distributors by:

- Managing and reporting vulnerabilities (Annex I, Section 2)
- Supporting technical documentation and risk assessments (Article 10)
- Ensuring compliance with certification and standards (Article 18)

Compliance with the CRA can be demonstrated through logs, technical reports, and risk management processes—services that SOCs are well-equipped to provide (Shaffique, 2024).

3.4.3 CSRD, ESRS S4, and SOC-generated reporting data

The Corporate Sustainability Reporting Directive (CSRD) (European Parliament, 2022) and European Sustainability Reporting Standard (ESRS S4) require companies to report how they manage risks affecting consumers and end-users, including data breaches. SOCs can contribute by:

- Providing evidence of implemented technical and organisational measures (GDPR Article 32, NIS2 Article 21)
- Supplying audit-ready documentation (logs, threat reports, incident records)
- Supporting management in risk governance and reporting (NIS2 Article 20)

Boggini (2024) demonstrates that compliance with GDPR and NIS2 directly enhances CSRD-aligned reporting and stakeholder transparency. External SOC services can significantly support organisations in meeting the requirements of EU cybersecurity legislation. SOCs contribute to:

- Fulfilling technical and organisational obligations (NIS2, CRA)
- Enhancing audit readiness and reporting quality (CSRD, ESRS)
- Supporting executive accountability and training (NIS2 Article 20)

Integrating SOC services into an organisation's cybersecurity strategy is an effective way to demonstrate compliance and build stakeholder trust.

4. Knowledge Base

This section provides a critical synthesis of existing literature. It combines methodologies, highlights research gaps, and evaluates relevance to the proposed governance model. The governance model proposed in this research is grounded in a robust and multidisciplinary knowledge base that integrates empirical evidence, scientific theory, and methodological rigour.

4.1 Empirical Foundations

The model is based on a selection of key empirical studies examining cybersecurity vulnerabilities, threat landscapes, and operational realities in the healthcare sector. Ewoh and Vartiainen (2024) provide a socio-technical overview of systemic vulnerabilities in healthcare environments, emphasising the interplay between human factors, legacy systems, and organisational complexity.

Vilakazi and Adebesin (2023) present a systematic analysis of cybersecurity threats and mitigation strategies, emphasising the prevalence of ransomware, phishing, as well as the importance of encryption and anomaly detection. Alzaabi and Mehmood (2024) present a comprehensive analysis of insider threat detection, emphasising the limitations of classical machine learning approaches and highlighting the promise of deep learning and NLP-based methods, particularly those leveraging large language models, for enhancing detection capabilities through contextual understanding and temporal pattern analysis.

Aijaz et al. (2023) evaluate threat modeling methodologies in the healthcare IT sector and provide insights into the applicability of structured methodologies for identifying and assessing cyber risks. Veriti (2025) report and the Health-ISAC annual threat report (Health-ISAC, 2025) provide up-to-date information on threat actor behaviour, attack vectors, and sector-specific vulnerabilities, highlighting the need for coordinated CTIS practices. These studies collectively underscore the necessity of integrating human, technical, and organisational dimensions into the design of CTIS governance frameworks.

4.1.1 Comparative critique

Ewoh and Vartiainen (2024) highlight socio-technical vulnerabilities in their article, emphasising human factors and organisational complexity. Vilakazi and Adebesin (2023) focus on technical migration strategies such as encryption and anomaly detection. In contrast, Alzaabi and Mehmood (2024) advocate advanced insider threat detection using deep learning and NLP.

Aljaabi's and Mehmood's article differs from Aijaz et al's argument, which prioritises structured threat modeling methods. These variations highlight the research tension between a proactive governance framework and reactive technical controls. There is also a gap in integrating governance models with adaptive technical solutions under strict EU regulatory constraints, and this study aims to address this.

4.2 Scientific Foundations

The theoretical foundations of the governance model emerge from several established scientific domains. Systems Theory provides a holistic perspective for understanding the dependencies between technological components, organisational processes, and external environments(Becker et al., 2023). Socio-Technical Theory emphasises the co-evolution of social structures and technical systems and advocates for design that balances usability, security, and institutional constraints (Malatji et al., 2019).

Information Systems Governance Models provide structured approaches for aligning IT operations with strategic goals, regulatory requirements, and risk management practices. Cyber Resilience Theory in healthcare describes a model's ability to anticipate, withstand, and recover from cyber disruptions, particularly in critical healthcare infrastructures (Salami, 2025).

4.3 Design Science and Methodological Tools

The model development process is guided by principles of Information Systems Design Theory, which supports the creation of purposeful, context-sensitive artefacts. It also incorporates:

- Governance Models that define roles, responsibilities, and decision-making structures for CTIS.
- Information Sharing Frameworks that facilitate secure, interoperable, and policy-compliant data exchange across organisational boundaries.

To ensure methodological rigour, the following tools and techniques are employed:

- Design Patterns that encapsulate reusable solutions to common design challenges in cybersecurity and information sharing.
- Evaluation Frameworks, including Realistic Evaluation and Case Analysis, which enable context-sensitive assessment of artefact effectiveness and stakeholder relevance.
- Information Systems Modeling Methods, such as Business Process Model and Notation (BPMN) and Unified Modeling Language (UML), which support the formal representation of workflows, system interactions, and governance structures.

Together, these elements form a comprehensive knowledge base that supports the design, implementation, and evaluation of a governance model for cyber threat information sharing in the healthcare sector under EU regulatory constraints.

5. Governance Model Design

The proposed governance model for cyber threat information sharing (CTIS) in the healthcare sector is designed to align technical capabilities with organisational processes and regulatory obligations. It builds upon the DYNAMO platform's architecture and integrates sector-specific governance adaptations, stakeholder roles, and evaluation mechanisms to ensure secure, compliant, and effective CTI exchange.

5.1 Roles and Responsibilities

The governance model defines clear roles for key actors involved in CTIS. The Security Operations Centre (SOC) and Computer Emergency Response Teams (CERT) are responsible for threat detection, response, and coordination across organisational boundaries. Data Protection Officers (DPOs) ensure compliance with data protection regulations such as GDPR and the Health Insurance Portability and Accountability Act (HIPAA).

Healthcare administrators oversee operational integration and policy implementation in clinical settings. Platform administrators, sector-specific administrative directors, and compliance officers (as defined in the DYNAMO pilot) support technical oversight, regulatory alignment, and ongoing monitoring. These roles are structured to support a phased implementation, including preparation, execution, and refinement, as outlined in the DYNAMO pilot strategy.

5.2 Information Sharing Processes

The governance model includes structured processes for secure and interoperable CTI data exchange. Secure communication channels are created using standardised protocols such as STIX/TAXII. Anonymisation protocols are monitored using tools such as the Data Anonymisation Tool (DAT), which applies NLP techniques to sanitise sensitive data. Escalation procedures are defined to ensure that detected threats are responded to quickly, and there are clear coordination paths between stakeholders. These processes are embedded in the DYNAMO platform's Early Warning System (EWS), which aggregates internal and external threat data and supports automated dissemination.

5.3 Compliance Mechanisms

To ensure regulatory alignment, the governance model integrates:

- Embedded compliance checks for GDPR, NIS2, CRA, and the AI Act.
- Policy frameworks that define trust groups, data handling rules, and sector-specific governance adaptations (e.g., HIPAA in healthcare, NERC-CIP in energy).
- Evaluation metrics such as CTI sharing effectiveness, governance adoption rate, and stakeholder trust index, which guide iterative refinement.

These mechanisms are validated through pilot testing, as described in the DYNAMO implementation framework.

5.4 Technology Integration

The governance model leverages the technical capabilities of the DYNAMO platform, including:

- Early Warning System (EWS) for threat detection and alerting.

- Correlation Engine for identifying relationships between threat indicators using rule-based and machine learning techniques.
- MISP and STIX 2.1 for structured data exchange and interoperability.
- Attribute-Based Encryption (ABE) for fine-grained access control.

To support modeling and implementation, the governance framework employs:

- Business Process Model and Notation (BPMN) for visualising workflows.
- Unified Modeling Language (UML) for system architecture and role interactions.
- Design Patterns and Evaluation Frameworks (e.g., Realistic Evaluation, Case Analysis) to guide artefact development and assessment.

Together, these components ensure that the governance model is not only theoretically sound but also practically viable, adaptable to sector-specific needs, and scalable across critical infrastructure domains.

6. Evaluation and Implementation Strategy

The governance model will be evaluated using realistic evaluation and case analysis in selected healthcare organisations. These methods allow for context-sensitive assessment of how well the governance principles translate into operational effectiveness, stakeholder trust, and regulatory compliance. Evaluation metrics such as CTI sharing effectiveness, governance adoption rate, and stakeholder trust index will guide iterative refinement.

To ensure scalability and sustainability, a phased rollout strategy is proposed:

1. Pilot testing in selected hospitals, where the governance model and DYNAMO tools are deployed in controlled environments to validate technical functionality and compliance mechanisms.
2. Regional integration with CERTs, enabling coordinated threat response and intelligence sharing across healthcare institutions and regional cybersecurity teams.
3. National deployment coordinated by health authorities, ensuring alignment with national cybersecurity strategies, regulatory frameworks, and public health priorities.

This staged approach supports continuous stakeholder engagement, empirical feedback collection, and adaptive governance refinement. These allow the model to evolve in response to sector-specific challenges and operational realities.

7. Conclusion

This study demonstrates that applying a Design Science Research (DSR) methodology provides a robust foundation for developing a governance model for cyber threat information (CTI) sharing in the healthcare sector. By integrating theoretical insights from systems theory, socio-technical theory, information systems governance, and cyber resilience, alongside empirical evidence and practical implementation frameworks, the proposed model addresses the multifaceted challenges of CTIS under EU regulatory constraints. The governance model is not only theoretically grounded but also operationally viable. It aligns with the technical capabilities of platforms such as DYNAMO, incorporates structured processes for secure and compliant information exchange. It defines clear roles and responsibilities for key stakeholders, including SOCs, CERTs, healthcare professionals, and ICT personnel. The model also embeds compliance mechanisms for GDPR, NIS2, CRA, and the AI Act, ensuring legal alignment across jurisdictions. A phased implementation strategy, beginning with pilot testing in hospitals, followed by regional integration with CERTs, and culminating in national deployment, supports scalability, stakeholder engagement, and iterative refinement. Evaluation through realistic assessment and case analysis ensures that the governance principles are validated in real-world contexts. Looking ahead, future research should focus on extending the model to support cross-border CTIS, integrating AI-assisted threat detection capabilities, and enabling dynamic compliance monitoring. These directions will further enhance the adaptability, resilience, and regulatory robustness of CTIS governance in healthcare and other critical infrastructure sectors. Ultimately, this work lays the groundwork for a scalable, secure, and regulation-compliant governance framework that strengthens cyber resilience and fosters trust-based collaboration across the healthcare ecosystem.

Acknowledgements

Acknowledgement is paid to the DYNAMO Project, funded by the European Union under grant agreement no. 101069601. However, views and opinions expressed are those of the authors only and do not necessarily reflect

those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.

Ethics declaration: Ethical clearance was not required for the research.

AI declaration: Keenious Plus was used to assist with literature searching in this work. Copilot was used only in a limited manner to assist with paraphrasing and idea generation during the writing process. No AI tools were involved in producing the core analysis, arguments, or conclusions. The author takes full responsibility for the originality, accuracy, and final content of the paper.

References

Aijaz, M., Nazir, M., & Mohammad, M. N. A. (2023). Threat Modeling and Assessment Methods in the Healthcare-IT System: A Critical Review and Systematic Evaluation. *SN Computer Science*, *4*(6), 714. https://doi.org/10.1007/s42979-023-02221-1

Alzaabi, F. R., & Mehmood, A. (2024). A Review of Recent Advances, Challenges, and Opportunities in Malicious Insider Threat Detection Using Machine Learning Methods. *IEEE Access*, *12*, 30907–30927. https://doi.org/10.1109/ACCESS.2024.3369906

Becker, A. H., Goode, C. H., Rivers, J. C., Tyler, M. W., & Becker, J. J. D. (2023). Shared Governance and Systems Theory: A Mixed Methods Study of Faculty Perceptions and Ideas. *Higher Education Politics & Economics*, *9*(2), 22–47. https://doi.org/10.32674/hepe.v9i2.5974

Boggini, C. (2024). Reporting cybersecurity to stakeholders: A review of CSRD and the EU cyber legal framework. *Computer Law & Security Review*, *53*, 105987. https://doi.org/10.1016/j.clsr.2024.105987

Chalkias, I., Yucel, C., Mallis, D., Rajamäki, J., De Vecchis, F., Hagstrom, P., & Katos, V. (2023). An Empirical Evaluation of Cyber Threat Intelligence Sharing in the ECHO Early Warning System. *Communications in Computer and Information Science Series [In Press]*, *1790*.

DYNAMO project. (2024a). *Initial prototypes of the cyber-threat intelligence gathering, extraction, sharing components and AI-based solutions* (Deliverable No. D4.1; p. 73). https://horizon-dynamo.eu/wp-content/uploads/2025/02/DYNAMO-RPT-D41-V2-0.pdf

DYNAMO project. (2024b, May 9). *Dynamic Resilience Assessment Method Including Combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors*. https://horizon-dynamo.eu/wp-content/uploads/2023/01/DYNAMO_Leaflet_web.pdf

European Commission. (2022). *Cyber Regulation Act (CRA)* (Regulation No. COM(2022) 454 final). European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0454

European Parliament. (2022). *Corporate Sustainability Reporting Directive* (Directive No. 2022/2464; p. 66). European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2464

Ewoh, P., & Vartiainen, T. (2024). Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review. *Journal of Medical Internet Research*, *26*, e46904. https://doi.org/10.2196/46904

Health-ISAC. (2025). *2025 Health Sector Cyber Threat Landscape* (Health Sector Cyber Threat Landscape No. 2025; p. 27). Health-ISAC, Inc. https://health-isac.org/wp-content/uploads/Health-ISAC_2025-Annual-Threat-Report.pdf

Hevner, A. R. (2007). A Three Cycle View of Design Science Research. *Scandinavian Journal of Educational Research*, *19*(2), 1–6.

Lahdenperä, J., Muhonen, J., & Rajamäki, J. (2022). How to Utilize E-EWS as a Tool in Healthcare. *European Conference on Cyber Warfare and Security*, *21*(1), 438–441. https://doi.org/10.34190/eccws.21.1.401

Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information and Computer Security*, *27*(2), 233–272. https://doi.org/10.1108/ICS-03-2018-0031

Salami, I. A. (2025). Modeling and Measuring the Cyber Resilience of Critical Healthcare Infrastructure against Ransomware: A Cyber-Physical Systems Risk Perspective. *Journal of Engineering Research and Reports*, *27*(5), 231–252. https://doi.org/10.9734/jerr/2025/v27i51504

Shaffique, M. R. (2024). Cyber Resilience Act 2022: A silver bullet for cybersecurity of IoT devices or a shot in the dark? *Computer Law & Security Review*, *54*(September 2024), 106009. https://doi.org/10.1016/j.clsr.2024.106009

Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives. *IEEE Communications Surveys & Tutorials*, *25*(3), 1748–1774. https://doi.org/10.1109/COMST.2023.3273282

Vandezande, N. (2023). Cybersecurity in the EU: How the Nis2-Directive Stacks Up Against its Predecessor. *Computer Law & Security Review*, *52*, 105890. http://dx.doi.org/10.2139/ssrn.4383118

Veriti. (2025). *The State of Healthcare Cybersecurity 2025* (p. 18) [Research Report]. VERIT, a Check Point Company. https://veriti.ai/wp-content/uploads/2024/12/The-State-of-Healthcare-Cybersecurity-2025-_-A-Veriti-Research-Report.pdf.

Vilakazi, K., & Adebesin, F. (2023). A Systematic Literature Review on Cybersecurity Threats to Healthcare Data and Mitigation Strategies. In A. Gerbera & K. Hinkelmann (Eds.), *EPiC Series in Computing* (Vol. 93, pp. 240–251). EasyChair. https://doi.org/10.29007/hf15