Aligning DYNAMO Framework with the EU Cyber Resilience Act in the Energy Sector

Ilkka Tikanmäki[1,2][1] Jarmo Maikkola[1], Joonas Nykopp[1], Petri Nyfors[1], Sara Väisänen[1] and Shakti Panta Khatri[1]

[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

Abstract: The importance of robust cybersecurity frameworks has been raised by the digitalisation of critical infrastructure, particularly in the energy sector. The European Union (EU) launched the Cyber Resilience Act (CRA) in 2022, establishing uniform cybersecurity standards for products with digital elements at all lifecycle stages to address this issue. CRA describes requirements for software and hardware products with digital elements placed on the EU market. This study examines the CRA's effects on the energy sector and evaluates how the DYNAMO platform can support compliance and enhance sectoral resilience. The platform's key element is a dynamic resilience assessment methodology, which combines business continuity management (BCM) and cyber threat intelligence (CTI). Significant cybersecurity vulnerabilities in the energy sector are identified in the study, which include a growing attack surface, complex supply chains, and convergence of operational technology (OT) and information technology (IT) systems. CRA's inability to address OT-specific challenges, particularly in legacy systems like SCADA, is highlighted in the study through a literature review and case study analysis. The gap analysis shows that although CRA follows standards like NIST and ISO 27001, it doesn't have provisions for real-time monitoring, adaptive risk management, and OT-specific protections. To resolve those gaps, the research suggests that DYNAMO include 24-hour incident reporting to the European Union Agency for Cybersecurity (ENISA), structured vulnerability disclosure protocols, and post-market surveillance mechanisms. Additionally, DYNAMO must develop customised plans for OT environments, which involve retrofitting outdated systems and improving threat detection abilities. The findings show that cybersecurity in the energy industry requires a more dynamic and functionally integrated approach. Aligning DYNAMO and CRA will support regulatory compliance and strengthen the industry's resilience to evolving cyber threats. The next stage of research should be to validate these recommendations via empirical testing and explore cross-sector applications of the DYNAMO framework.

Keywords: Cyber resilience act (CRA), Energy sector cybersecurity, Operational technology (OT), Critical infrastructure protection, Dynamo platform, post-market monitoring

1. Introduction

1.1 Background and Research Problem

The digitalisation of the critical infrastructure, especially the energy sector, has increased reliance on digital systems. The shift to more digital systems has exposed vulnerabilities in the energy sector and other critical infrastructure. This has made cybersecurity resilience an important part of comprehensive security. The European Union introduced the Cyber Resilience Act (CRA) in 2022 to establish uniform cybersecurity standards. CRA is a legal framework that describes requirements for software and hardware products with digital elements placed on the European Union market. These requirements cover the product lifecycle. (European Commission. Joint Research Centre, 2024)

The energy sector's strategic importance and its heightened vulnerability to cyber threats and regulatory complexities, examining how frameworks like the Dynamic Resilience Assessment Method Including Combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors (DYNAMO) project, align with CRA compliance, has become important so that compatibility with DYNAMO and CRA can be verified (DYNAMO project, 2024). DYNAMO is a dynamic resilience assessment method. It combines business continuity management (BCM) and cyber threat intelligence (CTI); these features can create a situational awareness picture and enhance organisational resilience. (DYNAMO project, 2024).

This study contributes to the growing body of knowledge on cybersecurity regulation and resilience of critical infrastructure by providing a comparative analysis of the EU Cybersecurity Act and the DYNAMO framework. It highlights regulatory gaps in the CRA, its limited coverage of operational technology, and suggests improvements to DYNAMO that would enable better alignment with CRA requirements. By combining business continuity management and cyber threat intelligence, the study presents a dynamic approach to resilience that

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

complements the static compliance mechanisms of the CRA. This dual perspective contributes to understanding how regulatory and operational frameworks can be aligned to improve cybersecurity in the energy sector.

Although CRA outlines mandatory cybersecurity measures across sectors (Szedlak, Reinemann and Hatzelmann, 2024), existing literature seems to lack a detailed analysis of how sector-specific frameworks, such as DYNAMO, align with CRA requirements - especially regarding unique challenges faced by the energy sector. This study addresses this gap by exploring CRA's practical implications for energy cybersecurity and evaluating how DYNAMO can effectively support regulatory compliance and resilience improvements.

Research questions of this study are:

RQ1: How does the Cyber Resilience Act (CRA) impact cybersecurity policies and resilience in the energy sector?

RQ2: How can existing frameworks like DYNAMO support compliance?

This study hypothesises that the CRA introduces stricter compliance measures expected to improve cybersecurity resilience in the energy sector, but implementation challenges may limit its full effectiveness. This study examines the requirements of the EU Cyber Resilience Act from the perspective of cybersecurity standards and cybersecurity risks.

This study addresses several pressing challenges in aligning cybersecurity frameworks with regulatory requirements in the energy sector. In the EU CRA, lifecycle-based cybersecurity obligations are primarily designed for IT systems, but they are not sufficiently covered for operational technology (OT), particularly legacy systems like SCADA. Real-time monitoring and adaptive response mechanisms are necessary in the energy sector due to the rapidly evolving threat landscape, which includes ransomware, supply chain attacks, and AI-based attacks. The formal compliance mechanisms and post-market monitoring capabilities required by the CRA are not present in existing frameworks like DYNAMO, even though they are strong in terms of resilience and situational awareness. By examining how DYNAMO can be improved to meet the CRA requirements, the study aims to improve regulatory compliance and operational resilience in critical energy infrastructures.

After the introduction, Section 2, a literature review, reviews the current state of the cyber environment and vulnerabilities in the energy sector, comparing the differences between DYNAMO and CRA using GAP analysis. Section 3 describes the methodology used. Section 4, Results, presents the research findings on cybersecurity threats in the energy sector and gaps concerning modern cyber threats. Finally, Section 5 summarises the results and provides recommendations for future research.

2. Literature

In the cyber threat landscape, the energy sector forms a high-risk target. The backbone of modern society is based on electricity, which sustains industry, households, and critical infrastructure such as healthcare and transport. In the energy sector, production, storage, and distribution are increasingly based on network- and software-based solutions, which is why they are exposed to vulnerabilities (ECSO, 2018). New technology also brings new types of threats, such as attack methods based on artificial intelligence. Also, the geopolitically unstable situation in the world increases the risk of large-scale and disruptive cyberattacks targeting the energy sector (World Economic Forum, 2025). Especially in the electricity sector, the resilience of the electricity ecosystem has been found, according to research, to be weak, and in addition, there is a shortage of cyber professionals on the market (Ruoslahti and Tikanmäki, 2022).

Cyberattacks have various consequences, such as impacts on the economy, national security, daily functions, and overall trust in society. Economically, attacks can cause significant damage, increase energy costs, and disrupt trade. An attack on energy infrastructure affects national defence and security policies. When household access to electricity becomes more difficult, daily services become more complicated, endangering citizens' safety and reducing the quality of life. In the long run, the unreliability of the energy system and frequent power outages erode trust among businesses and citizens in society’s stability.

CRA obligations include meeting security requirements relating to the properties of products with digital elements, such as ensuring the absence of any known exploitable vulnerabilities, providing secure-by-default configurations, and enabling the ability to address vulnerabilities through security updates. Additionally, they must comply with vulnerability handling requirements, which involve conducting regular testing and security reviews of the product. Manufacturers are required to manage and address vulnerabilities effectively for the expected lifetime of the product, or five years from the product’s placement on the market, whichever is shorter. (Schmitz-Berndt and Cole, 2022).

Ukraine's electricity grid was subjected to a cyberattack on 23 December 2015; the attack targeted three regional electricity companies in Ukraine. As a result of the attack, 225,000 customers were left without electricity for several hours. The attack took place at three different sites almost simultaneously, indicating a precisely planned and coordinated operation. The implementation of the attack included, among other things, a telephone denial-of-service attack, malicious firmware, the KillDisk destruction program, and the BlackEnergy 3 malware (Lee, Assante and Conway, 2016).

In the United States, the Colonial Pipeline company was subjected to a ransomware attack on May 7, 2021; behind the attack was the DarkSide group. The attack targeted the company's billing system. Approximately 45% of the gasoline and jet fuel on the U.S. East Coast flowed through the company's pipeline. The entire pipeline had to be shut down, which affected the lives of millions of people, airports, and airlines, resulting in increased gas prices, fuel shortages at gas stations, and panic. The company paid the group a ransom of 4.4 million dollars, part of which was recovered, but the company's brand suffered significant reputational damage. The attack's success was enabled by inadequate protection of multi-factor authentication, a basic cybersecurity tool against hackers (Ene and Savu, 2023). The CRA explicitly introduces a product lifecycle approach, recognising that technological products can evolve. They may become insecure or be used in new contexts, requiring continuous attention to cybersecurity.

3. Method

This study utilises a descriptive literature review and case study analysis. The descriptive literature review systematically examines existing research and reports (Kim, Sefcik and Bradway, 2017) related to the Cyber Resilience Act, cybersecurity frameworks, and threats in the energy sector. The case study method (Yin, 2009) provides detailed examinations of significant cybersecurity incidents, enabling an understanding of real-world impacts, vulnerabilities, and the practical implications of CRA compliance and implementation within critical energy infrastructures.

This study employs a qualitative research design involving a descriptive literature review and case study analysis to examine the connection between the Cyber Resilience Act (CRA) and the DYNAMO framework for energy cybersecurity. A systematic review of literature involves examining academic publications, EU regulatory documents, cybersecurity frameworks such as NIST (National Institute of Standards and Technology, 2018), ISO 27001 (ISO, 2022), and industry reports (Saeed *et al.*, 2023). Sources were selected based on their relevance to CRA implementation, energy sector vulnerabilities, and resilience strategies. The evaluation identifies gaps in CRA's operational technology (OT) coverage and assesses DYNAMO's response to these challenges.

Real-world vulnerabilities and the consequences of inadequate cybersecurity measures were illustrated through the analysis of two high-profile cyberattacks, the 2015 Ukraine power grid attack and the 2021 Colonial Pipeline ransomware attack. To mitigate similar threats, these cases are used to evaluate the practical applicability of CRA and the potential of DYNAMO. A gap analysis was done to compare CRA requirements and DYNAMO capabilities. The objective was to compare CRA's lifecycle security obligations to DYNAMO's BCM and CTI capabilities, and identify any overlaps, gaps, or potential improvements. The analysis concentrated on reporting incidents, post-market monitoring, and protections specific to the purpose.

4. Results

4.1 Cybersecurity Threats in the Energy Sector

In the energy sector, three essential characteristics expose companies to cyberattacks. The attack surface has increased because companies' operations and infrastructure have been spread over a wide geographical area. The actors in the field and their relationships with third-party supply chains are complex, exposing supply chains to supply chain attacks. The physical and digital infrastructures in the electricity and gas sector are interconnected, which results in the OT infrastructure and IT networks being exposed to attacks.(Ene and Savu, 2023). Table 1 describes types of attacks that target the energy sector.

Table 1. Types of attacks targeting the energy sector (Ene and Savu, 2023).

Type of attack	Description
Malware	Software affecting the computer
Web-based attacks	Website used as a tool
Social engineering	Psychological manipulation

Type of attack	Description
Denial-of-service attacks (DoS)	Disable the user's computer or network
Insider threats	Parties connected to the organisation's network
Cyber espionage and cyber warfare	Unauthorised user activity
Botnets	Devices infected with malware
Ransomware	Malware is preventing the victim from accessing data

Malware is any software designed to affect a computer and install itself without the user's permission. Web-based attacks are threats in which a website is used as a tool of cybercrime. Social engineering (e.g., phishing, spam) is a psychological manipulation in which the attacker poses as a trustworthy party to get the target to perform desired actions, such as revealing confidential information or granting access to an account and computer. Denial-of-service attacks (DoS) aim to temporarily or permanently disable the user's machine or network by making it unusable. Insider threats (e.g., careless employees) include all parties connected to the organisation who may have critical information about the organisation's security practices, data, and IT systems. Cyber espionage and cyber warfare are attacks that involve unauthorised user activity in which data or systems are stolen from individuals or organisations for financial, personal, political, or military gain. Botnets, in which all devices connected to the network are infected with malware, enable remote control of the devices. Ransomware means malware that prevents the victim from accessing critical data or systems by encrypting them until the victim pays a ransom (Ene and Savu, 2023).

4.2 Overview of the Cyber Resilience Act (CRA)

The CRA (Cyber Resilience Act) applies to products with digital elements, including any software or hardware product and its associated remote data processing solutions. Several obligations must be fulfilled both before and while placing a product with digital elements on the market. For example, manufacturers, importers, and distributors must ensure that the product is accompanied by appropriate instructions and information, provided in a language that is easy for users to understand, to guarantee safe usage. (Schmitz-Berndt and Cole, 2022).

Manufacturers should carry out a cybersecurity risk assessment for each product, considering the assessment throughout all stages of the product's lifecycle - from development to delivery and maintenance. This risk assessment plays a crucial role in helping manufacturers determine the "appropriate level of cybersecurity based on the risks" (European Parliament and of the Council, 2024, p. 68) and identify the specific cybersecurity measures, as prescribed by the CRA, that must be implemented for the product. By adopting a risk-based approach, the CRA promotes a regulatory framework that adapts requirements according to the level of risk, while ensuring a consistent and coherent method for regulating the underlying technology. (Shaffique, 2024).

As regards importers, the Act provides for the obligation to ensure compliance with the essential cybersecurity requirements set out in Annexe I of the Act. Importers must check that the manufacturer has carried out a conformity assessment, confirm that the technical documentation is available, and that the product bears the Conformité Européenne (CE) marking, provide the necessary contact details, and include user-friendly instructions and product information. (Kaminaris, 2025).

To ensure that users can respond promptly to security incidents, manufacturers should inform users about any such incident and, where applicable, provide details of corrective measures to mitigate its impact. This communication can be done, for example, by publishing relevant information on the manufacturer's website, or where the manufacturer can contact users and justified by the risks by reaching out to users directly. (Schmitz-Berndt and Cole, 2022).

4.3 CRA's Limitations

The CRA framework presents an organised approach to evaluate cybersecurity readiness for the energy sector, which, however, has considerable gaps in contemporary cyber threats. The periodic nature of the audit is one major limitation; real-time monitoring is what the energy infrastructure needs against threats that evolve quickly, such as ransom attacks and supply chain compromises. While the CRA does fit well with NIST and ISO 27001 compliance standards, they often focus on regulatory checkbox exercises that detract from real security effectiveness, thus creating blind spots against advanced persistent threats (National Institute of Standards and Technology, 2018; ISO, 2022). Above all, it is rather more designed from an IT perspective, neglecting unique vulnerabilities arising from operational technology (OT) environments, particularly legacy ICS/SCADA systems, which are very much in use in energy networks (Stouffer *et al.*, 2023). These deficiencies highlight the

importance of an ever-evolving CRA that exceeds the behavioural static measures of compliance and meets the dynamic state of the challenge for energy sector cybersecurity.

To improve CRA's efficacy, the energy sector shall integrate within the framework capabilities for continuous threat monitoring and adaptive risk management. This means building security modules specific to OT, establishing dynamic threat intelligence feeds, and conducting mandatory cyber war-gaming exercises to stress-test incident response plans. By closing these gaps, CRA can evolve from a compliance tool to an active, real-time cybersecurity operational tool for protecting critical energy infrastructure. The modernisation of the CRA alongside investigators, energy companies, and information security personnel would have to occur to keep pace with the fast-changing threats facing the energy sector. Improvements would enable CRA to assess not just resilience but also actively reinforce defences against new emerging cyber threats.

4.4 Key Implications of CRA and DYNAMO

The energy sector faces several strategic and operational implications due to the comparison between the CRA and the DYNAMO framework. Table 2 summarises the key implications of the CRA and DYNAMO frameworks, highlighting their respective strengths and limitations.

Table 2*:* Key implications of CRA and DYNAMO.

Aspect	Cyber Resilience Act (CRA)	DYNAMO Framework
Purpose	Regulatory compliance for products with digital elements	Operational resilience for critical infrastructure
Focus Area	IT systems and product lifecycle	IT + OT systems, situational awareness, and threat intelligence
Approach	Static, audit-based, lifecycle security	Dynamic, real-time monitoring and adaptive response
OT Coverage	Limited; primarily IT-centric	Designed to include OT, but needs enhancement for legacy systems
Incident Reporting	Mandatory 24-hour reporting to ENISA	Not currently integrated; recommended for future alignment
Post-Market Monitoring	Required throughout product lifecycle	Not built-in; suggested for integration
Compliance Mechanism	CE marking, conformity assessments, documentation	No formal compliance mechanism; focuses on resilience
Threat Intelligence	Not included	Core component (CTI)
Lifecycle Security	Mandatory	Not explicitly covered

The energy sector faces multiple challenges in cybersecurity strategy, regulatory compliance, and operational resilience due to the differences between the DYNAMO framework and the CRA. Legal accountability is ensured by the CRA's compliance-based approach, but real-time protection against evolving threats is not guaranteed. DYNAMO's design is focused on resilience and provides proactive defence, but does not have formal regulatory compliance. Energy companies can fulfil the CRA's requirements without being completely secure, or they can be resilient but not compliant, and both situations have risks. The CRA's OT system vulnerabilities that are common in energy infrastructure are ignored by its IT-centric focus. DYNAMO's ability to tackle OT threats is crucial but not yet fully developed.

Legacy systems are vulnerable without OT-specific measures, which increases the risk of attacks like those in Ukraine and the Colonial Pipeline. Rapidly evolving threats may prevent CRA from keeping up with its regular audits and lifecycle-based security. This gap can be filled by DYNAMO's dynamic threat intelligence if it is properly integrated. Modern energy systems require real-time monitoring and adaptive response; regulatory frameworks must adapt to support this. Security is a requirement of CRA throughout the product lifecycle, while DYNAMO offers situational awareness and continuity planning. A cybersecurity strategy that is both compliant and operationally sustainable could be created by combining both approaches.

CRA and DYNAMO implementation without integration could result in duplication of effort, inefficiencies, or coverage gaps for organisations. To ensure operational safety, a standardised approach is required to ensure regulatory compliance supports it instead of undermining it. Legal accountability and standardisation across the EU are ensured by the compliance-oriented structure of the CRA. The dynamic and complex threat landscape of the energy sector, particularly in operational technology (OT) environments, may be limited by its static nature and IT-centric focus. DYNAMO's approach is more adaptable and resilient, and it combines business continuity management (BCM) and cyber threat intelligence (CTI) to provide a real-time situational picture. The difference demonstrates the necessity for regulatory frameworks to expand beyond routine audits to include continuous threat monitoring and adaptive risk management.

CRA requires lifecycle security and post-market surveillance to keep product integrity intact. DYNAMO's functionality is strong, but it lacks formal mechanisms to guarantee lifecycle compliance and structured vulnerability disclosure. Energy organisations that exclusively use DYNAMO may face difficulties in meeting CRA's statutory obligations. This could lead to regulatory sanctions or reputational risks due to this difference. The CRA's limited focus on OT systems poses a significant risk because the energy sector's legacy infrastructure frequently lacks modern security features. Although DYNAMO has the potential to address OT-specific threats, further development is necessary to meet CRA's expectations. DYNAMO would benefit from the integration of OT-specific modules and reporting protocols, which would improve regulatory compliance and operational efficiency.

Fragmented implementation of CRA and DYNAMO may lead to inefficiencies or gaps in cybersecurity coverage. A harmonised approach that combines the regulatory rigour of the CRA with the operational agility of DYNAMO would provide a comprehensive cybersecurity strategy that would ensure both compliance and resilience in critical energy infrastructures.

5. Discussion and Conclusions

5.1 Summary of Results

The digitalisation of the energy sector and the shift to more digital systems have made cybersecurity resilience a more important part of comprehensive security. The energy sector forms a high-risk target that is crucial to modern life. Attacks against Ukraine’s electricity grid are an example of the threat that has become possible with digitalisation. CRA is the European Union's legal framework that is developed to help counter these threats.

DYNAMO combines BCM and CTI to enhance organisational resilience. However, DYNAMO lacks some aspects of the CRA framework: DYNAMO should establish a 24-hour reporting protocol to relevant authorities like ENISA, integrate post-market monitoring and develop strategies for OT environments.

A few recommendations should be integrated to align the DYNAMO more closely with the CRA. DYNAMO should integrate structured vulnerability disclosure protocols and 24-hour incident response mechanisms with the European Union Agency for Cybersecurity (ENISA). These core requirements under the CRA ensure rapid identification, communication, and resolution of cyber threats. DYNAMO would enhance its responsiveness and support a coordinated cybersecurity posture across critical infrastructure sectors by embedding these elements into its operational procedures.

There is a need for DYNAMO to address the specific cybersecurity challenges of operational technology (OT) environments and legacy systems, which are particularly prevalent in the energy sector (Stouffer *et al.*, 2023). Unlike newer information technology (IT) systems, these infrastructures often lack built-in security features and are difficult to update. Therefore, DYNAMO should develop tailored strategies that include retrofitting outdated systems, enhancing OT-specific threat detection, and implementing risk controls suited to hybrid IT-OT environments.

In addition, DYNAMO should incorporate active post-market monitoring throughout the lifecycle of digital products. This involves continuous evaluation of security status, timely deployment of updates, and proactive risk management even after products are deployed. Such practices are essential to meeting CRA’s expectations for lifecycle security and to maintain a resilient security posture over time.

Manufacturers must, without undue delay and in any event within 24 hours of becoming aware of it, notify the named authority of any actively exploited vulnerability contained in products with digital elements, as well as any incidents that impact the security of those products (Schmitz-Berndt and Cole, 2022).

5.2 Limitations of the Study

The study's reliance on a qualitative literature review and case study analysis may make its findings less generalizable. The selection and interpretation of publications can be biased when relying on secondary data sources, such as published reports and academic literature. Conceptual gap analysis between the CRA and DYNAMO frameworks is used in the study, but it does not provide quantifiable metrics to evaluate the effectiveness of DYNAMO in real-world compliance scenarios for CRAs. The rapid evolution of cybersecurity threats and regulatory updates can cause some findings to become time-sensitive, making them require ongoing review and adaptation.

5.3 Suggestions for Future Research

Future research should be directed at validating the proposed DYNAMO-CRA compliance strategies through pilot projects in energy sector organisations. Quantitative studies can determine how DYNAMO improvements impact incident response time, vulnerability management, and overall resilience. In addition, cross-sector applications of DYNAMO in healthcare, transportation, and water infrastructure could be explored. To address the dynamic nature of cyber threats, it would be valuable to investigate AI-based threat detection and automated compliance monitoring.

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. 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.

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

AI declaration: The paper's spelling was verified using the artificial intelligence tool.

References

DYNAMO project (2024) Dynamic Resilience Assessment Method Including Combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors. Available at: https://horizon-dynamo.eu/wp-content/uploads/2023/01/DYNAMO_Leaflet_web.pdf (Accessed: 24 January 2024).

ECSO (2018) Energy Networks and Smart Grids: Cyber security for the energy sector. Analysis November 2018. Brussels, Belgium: European Cyber Security Organisation, p. 19. Available at: https://ecs-org.eu/ecso-uploads/2022/10/5fdb2673903c6.pdf.

Ene, I.-E. and Savu, D. (2023) 'Cybersecurity - A Permanent Challenge for the Energy Sector', Romanian Cyber Security Journal, 5(1), pp. 107–119. Available at: https://doi.org/10.54851/v5i1y202310.

European Commission. Joint Research Centre (2024) Cyber resilience act requirements standards mapping: Joint Research Centre & ENISA joint analysis. Analysis EUR 31892. Luxembourg: Publications Office of the European Union, p. 69. Available at: https://data.europa.eu/doi/10.2760/905934 (Accessed: 12 August 2025).

European Parliament and of the Council (2024) Cyber Resilience Act. Regulation 2024/2847. European Union, p. 81. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847.

ISO (2022) 'ISO/IEC 27001 Standard – Information Security Management Systems'. Geneva, Switzerland: ISO/IEC. Available at: https://www.iso.org/standard/27001 (Accessed: 6 June 2023).

Kaminaris, S. (2025) Cyber Resilience Act: Horizontal cybersecurity requirements for products with digital elements. Available at: https://www.ey.com/en_gr/technical/tax/tax-alerts/cyber-resilience-act-jan-2025 (Accessed: 12 August 2025).

Kim, H., Sefcik, J.S. and Bradway, C. (2017) 'Characteristics of Qualitative Descriptive Studies: A Systematic Review', Research in Nursing & Health, 40(1), pp. 23–42. Available at: https://doi.org/10.1002/nur.21768.

Lee, R.M., Assante, M.J. and Conway, T. (2016) Analysis of the Cyber Attack on the Ukrainian Power Grid. Analysis. Washington, D.C.: E-ISAC, p. 30. Available at: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf.

National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity. Framework. National Institute of Standards and Technology, p. 55. Available at: https://doi.org/10.6028/NIST.CSWP.04162018 (Accessed: 7 June 2023).

Ruoslahti, H. and Tikanmäki, I. (2022) 'E-Skills in Cybersecurity', in A. Dziech, W. Mees, and M. Niemiec (eds) Multimedia Communications, Services and Security (MCSS 2022). Cham: Springer International Publishing, pp. 36–48. Available at: https://doi.org/10.1007/978-3-031-20215-5_4.

Saeed, S. et al. (2023) 'A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience', Sensors (Basel, Switzerland), 23(16), p. 7273. Available at: https://doi.org/10.3390/s23167273.

Schmitz-Berndt, S. and Cole, M. (2022) 'Towards an Efficient and Coherent Regulatory Framework on Cybersecurity in the EU: The Proposals for a NIS 2.0 Directive and a Cyber Resilience Act', Applied Cybersecurity & Internet Governance, 1(1), pp. 1–17. Available at: https://doi.org/10.5604/01.3001.0016.1323.

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), p. 106009. Available at: https://doi.org/10.1016/j.clsr.2024.106009.

Stouffer, K. et al. (2023) Guide to Operational Technology (OT) Security. Special Publication SP 800-82r3. Gaithersburg, MD: National Institute of Standards and Technology, p. 316. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf.

Szedlak, C., Reinemann, H. and Hatzelmann, S. (2024) 'Ensuring Cybersecurity Compliance: Assessing SME Awareness and Preparedness for the Cyber Resilience Act', in Proceedings of Conference on Industrial Engineering and Operations Management. 5th Asia Pacific Conference on Industrial Engineering and Operations Management, Tokyo, Japan: IEOM Society International, USA, p. 10. Available at: https://doi.org/10.46254/AP05.20240160.

World Economic Forum (2025) Fostering Effective Energy Transition 2025. Insight Report June 2025. Cologny/Geneva Switzerland: World Economic Forum, p. 71. Available at: https://reports.weforum.org/docs/WEF_Fostering_Effective_Energy_Transition_2025.pdf.

Yin, R.K. (2009) Case study research: Design and methods. 4th edn. Thousand Oaks, California: SAGE Publications Ltd.