Information Security Journal: A Global Perspective

ISSN: 1939-3555 (Print) 1939-3547 (Online) Journal homepage: www.tandfonline.com/journals/uiss20

Cybersecurity Risks and Defense for a European Energy Retail Business: A Case Study Using FMEA and Bowtie Incident Analysis

Mikko Suorsa & P. Helo

To cite this article: Mikko Suorsa & P. Helo (30 Apr 2025): Cybersecurity Risks and Defense for a European Energy Retail Business: A Case Study Using FMEA and Bowtie Incident Analysis, Information Security Journal: A Global Perspective, DOI: 10.1080/19393555.2025.2489421

To link to this article: https://doi.org/10.1080/19393555.2025.2489421

© 2025 The Author(s). Published with license by Taylor & Francis Group, LLC.

Published online: 30 Apr 2025.

Submit your article to this journal

Article views: 246

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=uiss20

INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE
https://doi.org/10.1080/19393555.2025.2489421

Taylor & Francis
Taylor & Francis Group

OPEN ACCESS Check for updates

Cybersecurity Risks and Defense for a European Energy Retail Business: A Case Study Using FMEA and Bowtie Incident Analysis

Mikko Suorsa and P. Helo

School of Technology and Innovations, University of Vaasa, Vaasa, Finland

ABSTRACT

The energy industry plays a critical role in powering economies and modern societies, making cybersecurity and resilience essential. This study explores cybersecurity risks and mitigation strategies in the energy retail sector by analyzing incidents in a European energy retail organization under the EU NIS 2 Directive from 2018 to 2023. The research identifies eight key cybersecurity risk categories and applies Failure Modes and Effects Analysis (FMEA) to each, providing detailed risk assessments and recommended defensive measures. Additionally, the study presents graphical cyberattack visualizations using the Bowtie model to enhance understanding of cybersecurity risks in energy retail. From a theoretical perspective, the findings offer a comprehensive view of these risks, grounded in real-world incidents. Practically, the analysis provides valuable guidance on cybersecurity risk management for energy retail organizations and critical infrastructure businesses, ensuring compliance with emerging cybersecurity regulations that mandate executive oversight within IT governance, regulation, and compliance functions.

KEYWORDS

Energy Retail Business; FMEA; Incident Analysis; Information Security; Risk Visualization

1. Introduction

1.1. Research motivation

Energy powers all modern life, making cybersecurity in the energy industry necessary for the world's critical infrastructures (Yusta et al., 2011). The energy retail business, which involves the sale of energy products and services to businesses and consumers, is an important cornerstone for delivering essential services to society (Directive (EU) 2022/2555, 2022), as nearly all societal processes depend on energy (Löschel et al., 2010).

Cybersecurity is the key resilience factor for energy retail companies (Azzuni & Breyer, 2017) and disruptions in energy retail operations may cause further cascading effects in other critical sectors such as emergency services, water, food, transportation, communications, finance and manufacturing (Gouglidis et al., 2018). Specific risks include infiltration and theft of confidential data, interruption of services, as well as damage to or disruption of infrastructure, and compromise of physical assets (Barichella, 2023).

Cyberattacks have significantly evolved over time, transitioning from minor criminal activities to sophisticated, state-sponsored cyberterrorism (Ang & Utomo, 2017), while cyberattacks targeting energy and utility companies have increased in frequency and sophistication. Major cybersecurity incidents in the energy industry can have national security implications and cease energy retail operations, causing significant financial losses, compromise of sensitive information, legal liabilities, and the harming of brand reputation (Falowo et al., 2022).

An example of a notable incident is the 2020 cyberattack on the Portuguese energy company Energias de Portugal (EDP), which resulted in the loss of 10 terabytes of sensitive information and considerable financial and reputational damage (SektorCERT, 2022). Further examples include cyberattacks against the power grid in Ukraine (cf. Whitehead et al., 2017) and the Bowman Avenue Dam in New York (cf. Hassanzadeh et al., 2020).

Given the need to protect energy infrastructure from cyber threats to ensure uninterrupted operations (Venkatachary et al., 2017), the safeguarding of energy services with regulatory requirements has become a global megatrend and a mission for every sovereign state (Haber & Zarsky, 2018). European laws protecting essential services from cyber

CONTACT Mikko Suorsa k83110@student.uwasa.fi School of Technology and Innovations, University of Vaasa, Vaasa, Finland

© 2025 The Author(s). Published with license by Taylor & Francis Group, LLC.
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

threats are the Directive on Security of Network and Information Systems (NIS Directive) (Directive (EU) 2016/1148, 2016) and its successor, the NIS 2 Directive, which entered into force in January 2023, after which EU Member States were required to transpose its provisions into national law. The NIS 2 specifically obligates energy retailers to have risk-based cybersecurity management and stringent incident reporting, backed by administrative fines (Directive (EU) 2022/2555, 2022).

Similar developments to the NIS 2 are the NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) standards (cf. Dolezilek & Hussey, 2011), the Australian Security of Critical Infrastructure Act (SOCI Act) (cf. Shah, 2023), and the Critical Infrastructure Protection Act in South Africa (cf. Calandro, 2020).

International standards are essential for managing cybersecurity risks in critical infrastructure. ISO/IEC 27001 is regarded as the de facto standard for information security management (Calder & Gerard, 2013), offering a technology-neutral framework for establishing an information security management system (ISMS) to mitigate risks (ISO/IEC 27001: 2022). ISO/IEC 27002 complements this by providing guidance on security controls (ISO/IEC 27002: 2022). Similarly, the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) offers a recognized approach to enhancing cybersecurity resilience (National Institute of Standards and Technology, 2024). For organizations handling customer data, ISO/IEC 27701 builds on ISO/IEC 27001, focusing on privacy protection and compliance (ISO/IEC 27701: 2019).

A risk-based approach is needed to safeguard the energy retail business from cyber threats (Azzuni & Breyer, 2017), because cybersecurity is fundamentally a risk management practice (Stewart et al., 2012) and a crucial component of organizational IT governance, risk management, and compliance (IT-GRC) function (Soomro et al., 2016). Successful IT-GRC requires learning from cybersecurity incidents to understand and mitigate their causes (Patterson et al., 2023).

However, concrete information about cybersecurity incidents is scarce (Maschmeyer et al., 2020), which is why the number of academic studies on the subject is limited (Eling & Wirfs, 2019). Therefore, more data about cybersecurity incidents is needed so that their causes, effects, and risk mitigation strategies can be studied and proposed (Al-Mhiqani et al., 2018) for energy retailers.

Failure Modes and Effects Analysis (FMEA) is a risk management methodology used to identify an organization's potential failure modes, along with their causes and effects (Asllani et al., 2018). Widely recognized in cybersecurity management, FMEA enables energy companies to identify and effectively mitigate cybersecurity risks in their operations (Akula & Salehfar, 2021). These risks are often very complex, necessitating improved techniques to understand attack patterns and their corresponding defense mechanisms (Staheli et al., 2014), where graphical visualization tools have proved useful (Moody, 2007).

In this paper, the terms "cybersecurity" and "information security" are used interchangeably. Cybersecurity is often used as an all-inclusive term (von Solms & van Niekerk, 2013). However, the literature typically distinguishes cybersecurity as referring to everything that is fully digital, whereas information security adds the physical dimension and refers to all information regardless of its form (von Solms & von Solms, 2018). For a complete list of abbreviations used in this article, please refer to Table A1 in the Appendix.

1.2. Research objectives and methods

This paper analyzes the information security incidents of a European energy retail company over a six-year period, from 2018 to 2023, categorizing them into specific cybersecurity risks. A Failure Modes and Effects Analysis is conducted to provide deeper insights into effective mitigation strategies for these risks. Additionally, the paper demonstrates the use of the Bowtie graphical

attack modeling and visualization technique, enhancing the understanding of cyber threats and corresponding defense measures within energy retail companies.

1.3. Research problem and questions

The research problem of this paper is to identify and explore the impacts of information security incidents and to provide effective measures to mitigate the risks in the energy retail business. More specifically:

- Research Question 1: What are the main cybersecurity risk categories for the energy retail business?
- Research Question 2: What are the cybersecurity failure modes, effects, and corresponding mitigation measures for the energy retail business?
- Research Question 3: How can graphical attack modeling techniques enhance cybersecurity risk management for the energy retail business?

1.4. Main contributions

From a theoretical perspective, this study addresses a significant gap by providing new insights into the cybersecurity risks faced by the energy retail sector, drawn from real reported incidents. It also demonstrates the value of visual cyber attack-defense modeling techniques.

In practical terms, the study guides energy retail companies and businesses managing critical infrastructure in strengthening information security practices and complying with emerging cybersecurity regulations. By identifying risks, understanding attack tactics, and enhancing controls, it offers valuable insights. The Bowtie model provides a layered visualization of threats, impacts, and preventive controls, assisting stakeholders and executives better understand complex risk scenarios and make informed decisions to address vulnerabilities effectively.

1.5. Paper organization

The remainder of the paper is structured as follows: Section 2 presents a literature review, and Section 3 outlines the study's research methodology. The results are presented in Section 4 and discussed in Section 5. Finally, Section 6 concludes the paper by presenting theoretical and practical contributions, along with the study's limitations and directions for future research.

2. Literature review

The literature review highlights a significant research gap in cybersecurity risk management within the energy retail sector, particularly when compared to the extensively studied areas of energy production, distribution, and other critical infrastructure industries. Table 1 provides an overview of the relevant literature, emphasizing this gap.

Despite the increasing cyber threats and regulatory demands, such as those imposed by the NIS 2 Directive, there is a lack of research specifically addressing the unique challenges faced by energy retailers. This study contributes to the literature by addressing these gaps and providing actionable insights for improving cybersecurity practices within the energy retail sector.

Cybersecurity risk management is widely recognized as essential across various critical infrastructure sectors. For instance, Ani et al. (2016) discuss its significance in manufacturing, Gioulekas et al. (2022) focus on healthcare, Shoetan et al. (2024) examine cybersecurity risks in telecommunications, and Almudaires and Almaiah (2021) explore challenges within the payment card industry. Additionally, Kulkarni et al. (2024) address cybersecurity incidents in food and agriculture, while Tuptuk et al. (2021) investigate water systems,

Table 1. Literature review.

Authors	Category	Study design	Purpose
Ani et al. (2016)	Manufacturing	Literature analysis of cybersecurity in industrial control systems	Trends in cybersecurity challenges and solutions in the manufacturing industry
Gioulekas et al. (2022)	Healthcare	Survey of cybersecurity culture	Proposed solutions to cybersecurity threats in the healthcare industry
Shoetan et al. (2024)	Telecommunications	Literature analysis	Proposal for enhancing telecommunications cybersecurity using artificial intelligence
Almudaires and Almaiah (2021)	Payment card industry	Analysis of major incidents	Cybersecurity risk mitigation solutions for payment card companies
Kulkarni et al. (2024)	Food and agriculture	Analysis of major incidents	Proposed solutions to cybersecurity threats in the food and agriculture industry
Tuptuk et al. (2021)	Water systems	Review of security in cyber-physical water systems	Future research directions in water systems cybersecurity
Melaku (2023)	IT-GRC	Literature analysis	Playbook for incident management
Patterson et al. (2024)	IT-GRC	Literature analysis	Research directions for cybersecurity incident analysis
Patterson et al. (2023)	IT-GRC	Interviews	Best practices for the cybersecurity incident learning process
Zhang et al. (2016)	Energy production	Visual analysis of selected cyberattacks	Proposal for a procedure to evaluate wind power system reliability
Lee et al. (2023)	Energy production	Analysis of selected cyberattacks and vulnerabilities	Proposal for a cybersecurity anomaly detection system for solar power plants
Zhang and Kelly (2022)	Energy production	Analysis of cyber risk assessment methods	Methods for evaluating cyber risks in nuclear power plants
Rajkumar et al. (2023)	Energy distribution	Analysis of major historical blackouts	Identification of cyber-physical incident factors in the power grid
Krause et al. (2021)	Energy distribution	Analysis of typical infrastructure and attack vectors	Proposal for a power grid defense strategy
Sun et al. (2018)	Energy distribution	Review of studies and solutions	Summary of state-of-the-art cybersecurity in the power grid
Nazari and Musilek (2023)	Energy industry	Literature analysis	Challenges and barriers in energy company cybersecurity
Govea et al. (2024)	Energy industry	Analysis of critical infrastructure networks	Artificial intelligence solutions to enhance cybersecurity in the energy industry
Chen et al. (2021)	Energy industry	Literature analysis	Proposal for a secure cloud-based service framework for the energy value chain
Nikolaou et al. (2023)	Energy industry	Vulnerability identification using the common vulnerability scoring system	Vulnerability identification and assessment framework for the energy industry
Gong and Lee (2021)	Energy industry	Analysis of threat indicators in metering infrastructure	Cyber threat intelligence framework proposal for improved energy cloud security
Zografopoulos et al. (2023)	DER solutions	Analysis of typical threats targeting DER assets	DER cyberattacks, their impacts, and mitigation strategies
Hseiki et al. (2024)	DER solutions	Analysis of the typical attack surface	Proposal for a cyber-resilient smart meter
Tuyen et al. (2022)	DER solutions	Review of cybersecurity in inverter-based smart power systems	Future research directions in DER cybersecurity
Pourmirza and Walker (2021)	DER solutions	Analysis of typical infrastructure	Categorization of cybersecurity challenges for electric vehicle charging stations

underscoring the need for comprehensive risk management strategies across these sectors.

2.1. Cybersecurity risk management within the IT-GRC function

Information security is fundamental to organizational risk management (Stewart et al., 2012) and is a core element of the IT governance, risk management, and compliance (IT-GRC) function (Soomro et al., 2016). Cybersecurity can only be effectively managed by linking digital resilience to organizational strategy (Mizrak, 2023), where the business objectives are aligned with an organization's IT operations (Osden & Lubbe, 2009).

Governance is the setting of organizational goals through policies and processes overseen by executives. Risk management identifies, assesses, and controls risks, while compliance

ensures ethical integrity, adherence to regulations, and alignment with company policies and procedures (Wright, 2019).

The success factors of IT-GRC include the regular review of information security policies and strategies to address existing vulnerabilities and emerging threats, as well as the fostering of a security-conscious staff and culture (Melaku, 2023). Consequently, the key IT-GRC cornerstone is the analysis of cybersecurity incidents (Patterson et al., 2023).

Systematic preparedness and prompt response are needed to effectively control cybersecurity incidents, which are typically sudden, and possibly serious; therefore, urgent containment and mitigation are routinely necessary (Onwubiko & Ouazzane, 2022). An example of a cybersecurity incident are malware-infected computers. After detection and analysis, these computers should be isolated, reinstalled, and integrated back into operation (Line et al., 2014).

Learning from cybersecurity incidents and addressing their causes are natural ways to mitigate the likelihood of similar future occurrences (Patterson et al., 2023). However, concrete information about information security incidents is limited (Maschmeyer et al., 2020), therefore academic efforts to provide novel information about cybersecurity incidents and risk management best practices are encouraged (Patterson et al., 2024).

2.2. Cybersecurity risk management of the energy retail business within the energy industry

The energy industry value chain includes the production, trading, transmission, distribution, and retail business of energy. Production converts fossil or renewable resources into electricity or heat, while energy trading manages price fluctuation risks in international markets. Energy is transported over long distances and distributed over the electrical grid, and finally, energy retail is the sale of products and services to businesses and private customers (Brown et al., 2019).

The importance of information security in energy production is critical due to the severe consequences of potential incidents (Bıçakcı & Evren, 2022) and is widely recognized in the literature. For example, a study by Zhang and Kelly (2022), provides recommendations for nuclear power plant cyber risk assessments. Another study by Lee et al. (2023) proposes a cybersecurity anomaly detection system for networked solar power plants, and a study by Zhang et al. (2016) assesses wind farm reliability through cyberattack simulation.

Similar to energy production, the cybersecurity challenges and solutions in energy distribution have been extensively studied (cf. Sun et al., 2018; Wang & Lu, 2013). Rajkumar et al. (2023) analyze cyber-physical factors in major historical blackouts, while Krause et al. (2021) address power grid challenges and propose a layered defense strategy with categorized measures, and Tufail et al. (2021) provide insights into cybersecurity detection and mitigation for the smart grid.

Studies on the entire energy industry often encompass the energy retail business, recognizing it as a prime target for cybercriminals because of its financial value (Dagoumas, 2019). Common challenges faced by energy retailers include scams, contract fraud (Chen et al., 2021), and a rising number of ransomware attacks that pose threats to operations, finances, and reputation (Dogan & Edwards, 2022).

The literature highlights cybersecurity and data privacy challenges faced by energy companies, particularly in relation to digital transformation and the large volume of customer data involved (Nazari & Musilek, 2023). Within the broader energy sector, Gong and Lee (2021) introduce a tool for generating cyber threat intelligence; Govea et al. (2024) offer artificial intelligence solutions to transform cybersecurity in the energy industry value chain; and Nikolaou et al. (2023) propose a model for identifying and assessing vulnerabilities in critical energy infrastructure network.

Distributed Energy Resources (DERs) are becoming universal in the energy industry, presenting significant cybersecurity needs (Zografopoulos et al., 2023), and are a popular research topic in the context of Industry 4.0

(Faheem et al., 2018). This is due to the interconnected, decentralized, and interoperable nature of DERs, as well as their typical remotely controllable features (Zografopoulos et al., 2023).

The literature on cybersecurity in DERs occasionally focuses on the customer interfaces of DER solutions. These include, for instance, solar panels, battery storage, electric vehicle charging stations (EVCS) (Zografopoulos et al., 2023), inverters (Tuyen et al., 2022), and smart meters (Hseiki et al., 2024).

A study by (Zografopoulos et al., 2023), provides insights into DER cybersecurity vulnerabilities, attacks, impacts, and mitigation strategies. Sun et al. (2020) propose mitigation measures for smart inverter cybersecurity threats, and Hseiki et al. (2024) address the cybersecurity vulnerabilities of smart meters. Pourmirza and Walker (2021) and Hamdare et al. (2023) analyze the cybersecurity risks and challenges specific to EVCS.

2.3. NIS 2 requirements to energy retail business

Safeguarding critical infrastructures through cybersecurity legislation has been a significant interest of the European Union (EU) since the early 21st century (Bederna & Rajnai, 2022). The first Directive on Security of Network and Information Systems (NIS directive) in 2016 was a milestone in establishing a unified level of cybersecurity within EU member countries (Vandezande, 2024).

Since then, the EU has commenced more cybersecurity proposals such as the European Cyber Resilience Act (CRA) (cf. Chiara, 2022) and the Network Code for Cyber Security (NCCS) for the electricity sector (cf. Skias et al., 2022). However, after the first NIS Directive, the EU member states still had different levels of cyber threat preparedness and uneven protection of consumers and businesses (Dragomir, 2021).

Improvements to the first NIS Directive were deemed insufficient due to expanded threats (Schmitz-Berndt, 2023). Consequently, the EU published its new cybersecurity strategy in 2020, which included a proposal to reform the Directive on Security of Network and Information Systems (NIS 2 Directive) that member states had to incorporate into their national legislation (European Commission, 2020).

Energy supply, transmission, and distribution were within the scope of the first NIS Directive (Directive (EU) 2016/1148, 2016). NIS 2 Directive expands this scope by distinguishing between essential entities and important service entities. Energy retailers are classified as an essential entity and need to comply with NIS 2 requirements (Directive (EU) 2022/2555, 2022).

NIS 2 mandates a risk-based information security management approach for energy retail companies. Key elements include risk analysis, incident management, business continuity, disaster recovery, and thorough supplier assessments, while the organizational management must approve and oversee the execution of these measures (Directive (EU) 2022/2555, 2022).

Incident management and prompt reporting to the authorities are fundamental NIS 2 requirements. Energy retail companies must report significant incidents that have caused or could cause harm to essential service delivery and notify service recipients of cyber threats (Directive (EU) 2022/2555, 2022). This obligation includes incidents considered significant, even if any damage has not yet been materialized (Schmitz-Berndt, 2023).

According to NIS 2, the organizational management can be held liable for violations of these requirements. Furthermore, NIS 2 enforcement includes administrative fines up to a maximum of 10 million EUR or 2% of worldwide turnover, whichever is higher (2022), underlining the importance of cybersecurity risk and incident management for energy retail companies.

3. Research methodology

In this section, the material for the single case study is presented, along with the methods used: Failure Modes and Effects Analysis (FMEA) and Bowtie analysis.

3.1. Material of the study

The case organization of this study is a European energy retail company. The study material consists of the cybersecurity incidents internally reported by the case organization over the six years from 2018 to 2023.

3.2. Single case study design

This study employs a single case study method, chosen specifically to analyze cybersecurity risks and mitigation strategies in the energy retail sector within its real-world context. Single case studies are comprehensive analyses and representations of a single unit or system within a specific context and time (Hancock et al., 2021).

The chosen approach provides rich and qualitative data that is essential for theory generation in complex areas (Eisenhardt, 1989) and allows for a detailed exploration of the phenomenon (Yin, 2018). The single case study approach captures nuances that may be overlooked in larger studies, particularly in unique settings (Eisenhardt, 1989), and is valuable for addressing research gaps, in previously unexplored areas (Yin, 2018).

The hallmark of case study research is the clear statement of theoretical arguments and the rich presentation of evidence in tables and appendices. The result produces fresh, new information that adds thorough evidence to conventional deductive research (Eisenhardt & Graebner, 2007), while further case study benefits include exploring design opportunities and demonstrating the use of novel tools (Lazar et al., 2017).

Case studies can be intrinsic, applied to specific scenarios, or instrumental, generating broader insights. They can also be embedded, where multiple sub-units within a case are studied, or holistic, where a single entity is studied as a whole (Brereton et al., 2008).

Case studies are criticized for lacking precision, objectivity, and rigor compared to larger studies. To address this, researchers should define the significance of their research questions and explain why current theories are incomplete. Another challenge is case selection, because readers may expect generalizations. The response is to clarify that the goal is not to test but to develop new theories (Eisenhardt, 1989; Eisenhardt & Graebner, 2007).

Dooley (2002) highlights the need to ensure a replicable line of evidence by describing the data gathering and analysis techniques, as well as using various methods to uncover unintended outcomes. Furthermore, to produce

Table 2. Case study protocol.

ID	Element	Purpose	Description
1.1	Background	A review of previous research to identify and highlight the research gap	Limited information on incident-based cybersecurity risks for energy retailers, their corresponding risk management measures, and risk visualizations using graphical attack modeling techniques
2.1	Design	A description of whether the case is intrinsic or instrumental	An instrumental study that generates broader insights
2.2	Design	A description of whether the case is embedded or holistic	A holistic study in which the single entity is examined as a whole
3.1	Case selection	A description of the criteria for case selection	A European energy company with a retail business operating under the EU NIS 2 directive across multiple countries, offering electricity and DER products to both private and business customers
4.1	Data collection	A description of the data collected	The data consist of information security incidents formally reported through the case organization's internal incident reporting system, with data extracted from the system for the years 2018 to 2023
5.1	Analysis	A description of the criteria used for data analysis	Incident data were aggregated into groups, forming the primary cybersecurity risk categories addressed in research question 1, along with their subcategories, which are addressed in research question 2, using FMEA analysis. The controls described to mitigate these risks in each FMEA analysis represent typical examples of how cybersecurity risks can be managed. Two risk examples are visualized using the Bowtie analysis method, in response to research question 3
6.1	External validity	A description of the domain to which the study findings apply	Research on cybersecurity risk management within the IT-GRC domain of the energy retail business, explored through studies of the energy industry value chain
7.1	Reporting	An overview of the target audience	Information security researchers and industry professionals in the energy retail sector, especially those involved in the IT-GRC value chain of the energy industry, as well as businesses safeguarding critical infrastructure

a rigorous case with greater validity, Eisenhardt (1989) and Yin (1994) both emphasize the use of a case study protocol to guide all elements of case research. The case study protocol in Table 2 of this study is adapted from Brereton et al. (2008).

3.3. Failure modes and effects analysis

This study employs Failure Modes and Effects Analysis (FMEA), which is a widely used method for analyzing and managing cybersecurity risks (Asllani et al., 2018). Applying FMEA is part of the larger trend of integrating cybersecurity into traditional process hazard analysis methods, originating from the manufacturing industry (Cormier & Ng, 2020).

FMEA was first introduced by the US military in the 1940s, then adopted by the aerospace industry in the 1960s, and further used by Ford in the 1970s to improve automotive production and design. Today, FMEA is widely used across various industries to manage risk and enhance customer satisfaction (Sharma & Srivastava, 2018).

FMEA is a technique that uses spreadsheets to collect data and analyze results (Babeshko & Giandomenico, 2023). Its primary outcome is the recognition of potential failure modes, their causes and impact, and determining controls to mitigate risks and reduce costs (Akula & Salehfar, 2021). FMEA facilitates the identification and correction of potential weaknesses, thereby reducing the likelihood and impact of failures (Asllani et al., 2018). Table 3 illustrates the FMEA elements, as described by Carlson (2012).

In the literature, FMEAs are frequently customized to meet specific research needs in IT-GRC risk assessment, as demonstrated by Subriadi and Najwa (2020). In other studies, Asllani et al. (2018) developed C-FMEA for airport cybersecurity, while Zarreh et al. (2019) applied a modified FMEA utilizing game theory to assess cyber-physical threats in manufacturing systems. A limitation of FMEA is its inability to describe the interactions between failure modes when other types of analysis methods such as graphical attack modeling techniques can supplement them (Carlson, 2012).

3.4. Bowtie analysis among graphical attack modeling techniques

Graphical attack modeling techniques are used to visualize the sequence and combination of events that lead to a successful cyberattack. The attack tree is one of the most applied methods presenting cyberattacks in a bottom-up visual hierarchical structure, using shapes or plaintext (Lallie et al., 2020). The fault tree method shares a similar structure but has a standardized symbolic representation (ISO/IEC 61025: 2006).

The advantage of attack trees is their visual and self-documenting nature, which enables easy interpretation. However, their disadvantage is the difficulty of specifying all attacker actions and their interactions with various defensive countermeasures preventing attacks from being successful or limiting their impact (Nagaraju et al., 2017). An example of an attack tree adapted from Lallie et al. (2020) is illustrated in Figure 1.

As a response to the disadvantage of attack trees being unable to model the defender's countermeasures, attack-defense trees were proposed to include the visualization of these interactions (Kordy et al., 2010). An example of an attack-defense tree, with its core elements adapted from Ji et al. (2016), is illustrated in Figure 2.

Table 3. FMEA elements.

ID	Potential failure mode	Potential effects of failure	Potential causes	Typical prevention controls	Typical detection controls
1.	Description of the main objective of how the element is expected to operate				
1.1	Description of how the element fails to meet its intended functions and requirements	Descriptions of the consequences of the failure	Description of the specific reasons for the failure	Actions to reduce the likelihood that the failure will occur	Controls that react to faults during operations, reducing the impact of failure

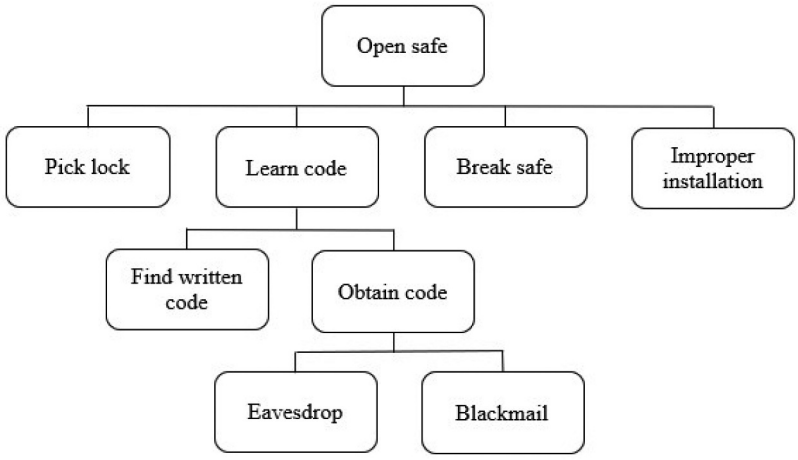

Figure 1. Example of attack tree.

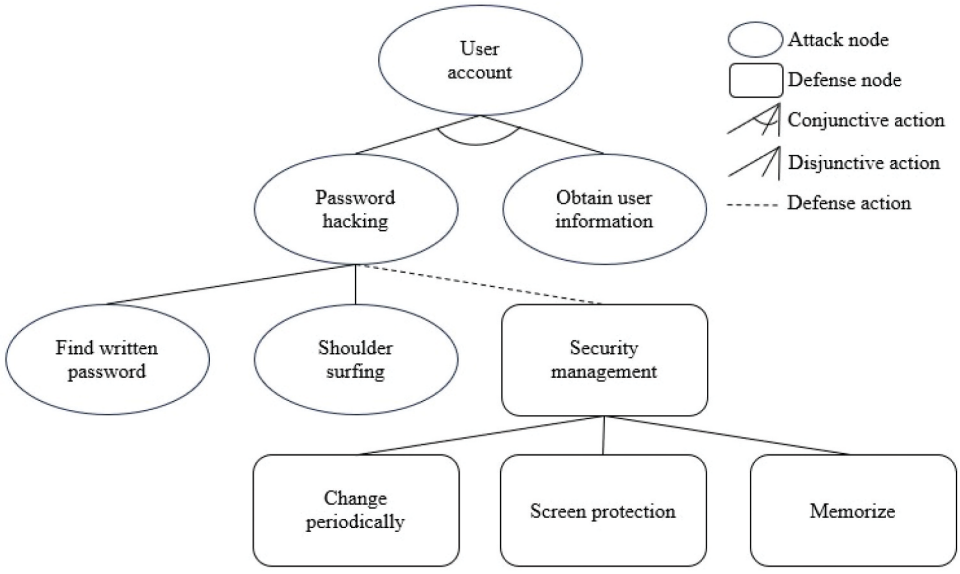

Figure 2. Example of attack-defense tree.

The bowtie analysis method is a more advanced graphical attack modeling technique for visualizing cybersecurity risks (Bernsmed et al., 2018), originally used in the 1970s for managing health, safety, and environmental hazards (Lewis & Smith, 2010). The "bow-tie approach" illustrates the relationships between threats and their consequences, along with layered protection measures (Markowski & Kotynia, 2011), to minimize business impact and damage (Lewis & Smith, 2010).

Bowties are useful for incident analysis, as they can detail multiple levels of causes and effects (Chevreau et al., 2006), which makes them a practical tool for visualizing cybersecurity risks (Bernsmed et al., 2018). No model will ever fully capture the complexity of reality; however, bowties are advantageous for increasing the understanding of risks among an intended audience (de Ruijter & Guldenmund, 2016) such as top management and executives.

The bowtie method has already been applied to cybersecurity research. Tøndel et al. (2020) used the bowtie in a study of electric power systems, while Wen and Faisal (2023) analyzed cyber incidents with bowtie in industrial control environments. Another study by Abdo et al. (2017) utilized bowtie for cybersecurity and safety scenarios in a chemical facility. The elements of the bowtie method are shown in Figure 3.

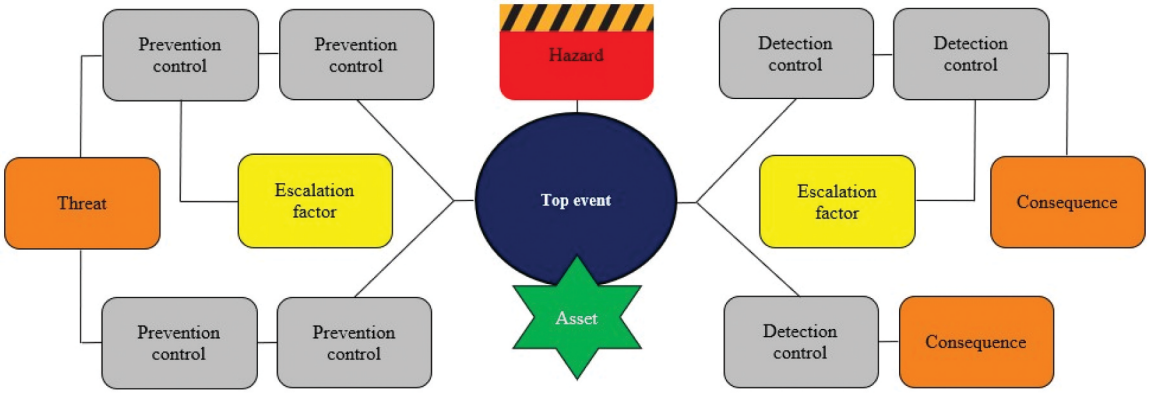

Figure 3. Elements of the bow-tie method.

In the bow-tie method, a hazard represents a potential risk that could lead to negative outcomes for valuable assets, such as data, systems, processes, employees, or infrastructure. The top event is the undesirable outcome that occurs if the hazard materializes. For example, a hazard could be a phishing attack targeting employees, and the top event might be unauthorized access to sensitive company data. Threats are factors that can trigger this top event, such as external attacks, system failures, or human error. Prevention controls are measures designed to stop these threats from occurring, acting as barriers to protect the asset (Meland et al., 2019).

Additionally, an escalation factor is a specific threat that can bypass or weaken defense controls, making the original threat more powerful or likely to occur. If the top event happens, it can lead to consequences such as damage, loss, or disruption. Detection controls are implemented to manage these outcomes. These reactive measures are activated only after the top event takes place, helping to minimize or prevent further damage and harm (Meland et al., 2019).

4. Results

This section presents the analysis results and answers to the research questions. Section 4.1 provides a high-level overview of the main cybersecurity risk categories for the energy retail business, while Section 4.2 offers a more detailed examination of the risks, with descriptions of failure modes, effects, and typical mitigation recommendations. Section 4.3 presents two examples of graphical visualizations of cyberattacks using the bowtie model.

4.1. Main cybersecurity risk categories for energy retail business

Analysis of the cybersecurity incidents internally reported by the energy retail case organization during the six years from 2018 to 2023 resulted in eight main cybersecurity risk categories. These are shown in Table 4.

The first risk category concerns energy retail companies' resilience against socially engineered phishing attacks. Phishing attackers aim to deceive users by impersonating trusted entities

Table 4. The main cybersecurity risk categories for energy retail business.

ID	Main cybersecurity risk category
1	The company is not resilient against socially engineered phishing attacks
2	The company's information systems are not resilient against cyberattacks
3	The company's change management controls are not maintained to ensure information security
4	The company's access controls are not managed to ensure information security
5	The company does not recognize and control the potential insider threat
6	The company does not ensure data protection compliance to protect customers' personal information
7	The company's supply chain does not adhere to the company's information security requirements
8	The company does not manage physical security to ensure employee safety and information security

in electronic messaging channels (NIST SP 800-82r3, 2023) in order to obtain sensitive information, perform financial fraud or install malware, potentially causing further cascading effects. Targets range from all users to specific groups or high-level executives (Stewart et al., 2012).

The second risk category concerns the resilience of information systems against cyberattacks, including denial of service (DoS), brute force, port scanning, injection, and ransomware attacks. The objective of DoS attacks is to prevent authorized system access or delay critical operations and functions by overwhelming the system with excessive requests (NIST SP 800-82r3, 2023). Injection attacks aim to compromise databases by introducing unexpected input or injecting malicious scripts into websites (Stewart et al., 2012).

A brute force attack tests all possible password combinations to gain unauthorized access (Garfinkel, 2015). Port scanning is often a precursor to an attack, used as a reconnaissance technique to examine active network hosts for vulnerabilities, facilitating further compromise attempts (Stewart et al., 2012). Ransomware is malware designed to encrypt data and prevent access unless a ransom is paid. Widespread ransomware attacks and their impacts, including significant data loss and financial damage, have contributed to its notoriety (Paquet-Clouston et al., 2019).

The third risk category relates to shortcomings in change management, which is a common cause of information system failures. Ineffective management in this area can result in a loss of oversight over system integrity, leading to unavoidable data breaches and the compromise of information confidentiality (ISO/IEC 27002: 2022).

The fourth risk category is access control management, a fundamental element of information security. Shortcomings in this domain are a common cause of data breaches, leading to excessive, unwarranted, and potentially malicious access to information, with possible further cascading consequences. Notably, inadequate access controls are often associated with insufficient records of user activities, meaning that illegitimate users cannot be held accountable for their actions (Suorsa & Helo, 2023).

The fifth risk category involves the recognition and further risk-based control of possible insider threats. The threat presented by malicious insiders is often underestimated, because insiders have intimate knowledge of valuable data and the means to access it (Stewart et al., 2012).

The sixth risk category concerns compliance with data protection laws. This category is highly important because energy retailers serve the end customer within the energy industry's value chain, processing significant amounts of their data in daily operations. A notable privacy law in Europe is the General Data Protection Regulation (GDPR), which lays out strict requirements for how organizations can process personal data to protect the privacy of EU citizens. Authorities enforce GDPR with large monetary sanctions (European Parliament & Council of the European Union, 2016) which increases the constant need to comply with the regulatory requirements.

The seventh risk category is supply chain cybersecurity for energy retail companies. The complex risks involve vendor system infiltration through the exploitation of third-party vulnerabilities, which can lead to significant data breaches, disrupted operations, legal disputes, reputational damage, and financial losses (Melnyk et al., 2021).

The eighth risk category addresses the physical dimension of ensuring employee safety and the security of information. Above all, the most important aspect of cybersecurity is protecting people from harm (Stewart et al., 2012). Numerous physical security areas of energy retail companies are access controls to company premises, secure handling of devices and storage media, adherence to clear desk rules, and safe disposal of assets.

4.2. Failure modes, effects, and corresponding mitigation measures for energy retail business

A Failure Modes and Effects Analysis (FMEA) was conducted for the main cybersecurity risk categories presented in the previous section. As a result, an FMEA table is provided for each category, along with recommendations for typical mitigation measures tailored to the energy retail business.

Table 5 displays the results of the first FMEA analysis, highlighting user awareness as the key

Table 5. FMEA for resilience against socially engineered phishing attacks.

ID	Potential failure mode	Potential effects of failure	Potential causes	Typical prevention controls	Typical detection controls
1.	The company is resilient against socially engineered phishing attacks				
1.1	Employees are not sufficiently aware of the types, hazards, and proper responses to phishing attacks	• Extraction of sensitive information • Installation of malware • Execution of financial scams • Failure to report phishing incidents	• Insufficient phishing training and awareness • Inadequate reporting process	• Awareness training on phishing types and dangers • Phishing reporting process • Tailored training for executives and users with privileged access • Spam filters • Phishing simulation campaigns • Software for phishing reporting and analysis	• Phishing simulation campaigns • Software for phishing reporting and analysis
1.2	Supply chain and customers are not aware of phishing attacks that exploit the company's identity	• Suppliers and customers are susceptible to phishing attacks that exploit the company's identity • Suppliers and customers are targeted by phishing attacks that exploit the company's identity	• No warnings issued to the supply chain and customers about phishing attempts using the company's identity • Delayed removal of fraudulent domains for web spoofing using the company's identity	• Reminders to the supply chain and customers about phishing attempts exploiting the company's identity • Instructions for handling fake domains that exploit the company's identity, including the use of domain takedown services	• Employee awareness of suspicious domains • Monitoring and blocking domains that impersonate the company's identity
1.3	Websites are vulnerable to URL redirection attacks	• Users accessing legitimate company websites are redirected to illegitimate sites, leading to phishing attacks, malware distribution, or interception of sensitive information	• Lack of up-to-date security controls to protect information systems and software	• Maintenance of up-to-date security controls on information systems and software • Domain Name System Security Extensions (DNSSEC) • Web application firewalls • Website scanners to identify vulnerabilities and malware	• Web application firewalls • Website scanners to identify vulnerabilities and malware

control in preventing successful phishing attacks that involve a significant social engineering component. This differentiates phishing from other types of cyberattacks because technical controls alone, such as spam filters, do not capture all malicious communications.

Protection against socially engineered phishing goes beyond technology, as it depends on end-user behavior (Abroshan et al., 2021). Therefore, it is important to ensure that staff members are aware of phishing types, associated risks, and reporting procedures. Tailored awareness programs for specific employee groups, such as executives and users with privileged access rights, along with simulated phishing exercises and phishing reporting software, should be implemented to maintain awareness and detect phishing attempts.

The company's supply chain and customers are also targeted by phishing attackers who exploit the company's identity. Therefore, suppliers and customers should be reminded of this risk, and measures should be taken to detect and take down fake domains used for fraudulent communications exploiting the company's brand name. Employee awareness is again important in detecting suspicious-looking domains, while monitoring tools can also be used to detect them.

Furthermore, from a technical standpoint, it is necessary to maintain up-to-date security controls on information systems and software to prevent the company's websites from being vulnerable to URL redirection attacks. Blocking access to domains distributing malicious content is the natural step (ISO/IEC 27002: 2022), while further controls include Domain Name System Security Extensions (DNSSEC), to sign domains for authenticity digitally, web application firewalls to filter and monitor traffic at the application level, and website scanners to identify vulnerabilities and malware.

Table 6 presents the results of the second FMEA analysis. The key to achieving cyber attack-resilient information systems is the continuous governance of the company's Information Security Management System (ISMS) based on standardization and control frameworks such as ISO/IEC 27001 or the NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) supported by continuous auditing and risk-based improvement actions.

Port scanning is prevented by closing inactive ports and configuring stateful firewalls to allow only necessary and context-based traffic. Network Address Translation (NAT) can also be applied to remap and conceal IP addresses, while Demilitarized Zones (DMZ) act as a buffer and a layer of defense between the internal network and the public internet. Intrusion Detection and Prevention Systems (IDPS) should be employed to enhance application security, while honeypots and honeynets divert and deceive malicious actors, and traffic logs should be analyzed for further mitigation (ISO/IEC 27002: 2022). Regular network audits prioritize the fixing of vulnerabilities to maintain up-to-date network security.

Measures to detect and restrict Denial of Service (DoS) attacks are primarily technical. Intrusion prevention systems, network devices for routing, switching, and load balancing, along with packet inspection, are used to identify and block DoS traffic. During a DoS attack, bandwidth throttling and rate limiting reduce internet speed to manage congestion, whereas content delivery networks further distribute traffic across servers. Redundancy and failover support continuous service by employing multiple systems and automatic switching during DoS attacks.

Injection attacks can be prevented by maintaining secure systems, protecting databases, and following secure development practices. The least privilege principle should be enforced to grant users only necessary access to systems and databases. Structured query language to prevent injection attacks can be achieved through input validation, sanitization, and whitelisting should be applied to ensure that user-provided data is accurate, matches predefined criteria, and is free from potentially harmful queries (ISO/IEC 27002: 2022). Additionally, errors and exceptions should be logged for further analysis. Auditing, security testing, and code reviews reveal vulnerabilities, whereas educating staff on secure practices creates awareness to prevent and detect these flaws.

Table 6. FMEA for cyberattack resilience.

ID	Potential failure mode	Potential effects of failure	Potential causes	Typical prevention controls	Typical detection controls
2.	The company's information systems are resilient against cyberattacks				
2.1	Vulnerabilities in information systems, software, and the company network	• Successful cyberattacks can cause disruptions to company operations, financial losses, theft of information, legal liabilities, and damage to reputation	• The security of information systems, software, and the company network is not adequately maintained	• Information Security Management System (ISMS) • Information security control and standardization frameworks, such as ISO 27001 or NIST CSF • Regular ISMS audits • Risk-based information security improvement cycle	• Regular ISMS audits • Risk-based information security improvement cycle
2.2	Insufficient measures to prevent port scanning	• Open ports and vulnerabilities in the network expose active hosts to potential attacks • Increased risk of targeted attacks • Reduced speed due to higher traffic volume	• Unused and open ports are vulnerable to port scans • The company's network security is not adequate to prevent port scanning	• Closure of unused ports • Stateful firewalls for context-based traffic decisions • Intrusion Detection and Prevention Systems (IDPS) • Demilitarized Zones (DMZ) • Honeypots and honeynets • Regular network audits	• Stateful firewalls for context-based traffic decisions • Intrusion Detection and Prevention Systems (IDPS) • Honeypots and honeynets • Log analysis • Regular network audits
2.3	Insufficient measures to prevent denial of service attacks	• Successful denial of service causes loss of information availability, disrupts business operations, and results in financial losses	• Measures to detect and restrict DoS traffic not implemented adequately	• Intrusion Detection and Prevention Systems (IDPS) • Bandwidth throttling and rate limiting • Routers, switches, and load balancers configuration • Content Delivery Network (CDN) • Packet inspection • Redundancy and failover mechanisms	• Intrusion Detection and Prevention Systems (IDPS) • Routers, switches, and load balancers configuration • Packet inspection
2.4	Insufficient measures to prevent injection attacks	• Successful injection attack leads to unauthorized access, data manipulation, system compromise, and breach of sensitive information	• Databases not protected adequately • Secure development practices not followed	• Up-to-date system security • Least privilege principle • Input validation, sanitization, and whitelisting • Error handling and exception logging • Security audits, testing, and code reviews • Security awareness training for key personnel	• Error handling and exception logging • Security audits, testing, and code reviews • Security awareness training for key personnel
2.5	Insufficient measures to prevent brute force attacks	• Successful repeated login attempts lead to compromised accounts, systems, and customer portals, with further cascading effects including phishing, the spread of malware, and theft of sensitive information	• Weak password and access control management measures	• Strong password policy with strong authentication • Account lockout and rate limiting • Verification of human users • Security awareness training for key personnel	• Access logging • Anomaly detection with behavioral analytics • Real-time alerting • Auditing of login attempts, lockouts and access patterns
2.6	Insufficient ransomware prevention and recovery measures	• Successful ransomware attacks have severe effects, including the encryption, theft and disclosure of sensitive information, operational disruption, legal and reputational damage, and financial loss	• Shortcomings in measures against phishing and cyberattacks • Lack of backup and disaster recovery plans	• Information Security Management System (ISMS) • Security culture initiatives • Staff training and awareness • Network segmentation • Disaster recovery plan • Secure backup strategies	• Information Security Management System (ISMS) • Security culture initiatives • Staff training and awareness • Real-time behavioral analysis • Sandboxing • Threat intelligence solutions

Measures based on a strong password policy should be enforced to prevent successful brute-force attacks supported by regular audits to identify weaknesses in its implementation (ISO/IEC 27002: 2022). Account lockout prevents access after several failed login attempts, while rate limiting restricts excessive access requests within a specified timeframe. Human user verification helps ensure that login attempts are made by humans, and not by automated software. Logs regarding successful and failed login attempts should be maintained for traffic pattern analyses, whereas the anomaly detection with real-time alerting can be used to identify and respond to unusual login activities.

To prevent and protect from ransomware attacks, a strong security culture supporting comprehensive cyber hygiene is necessary against cyberattacks, phishing, and malware. These are promoted by systematically managing the Information Security Management System (ISMS) through continuous staff training and awareness programs. A disaster recovery plan (DRP) is an obligation for readiness against severe cyberattacks. The DRP includes the maintenance of secure backups, operational restoration procedures, and regular testing of the plan with company management.

Effective ransomware detection involves real-time behavioral analysis of unusual traffic and sandboxing to isolate suspicious content. Segmented networks help limit the spread of ransomware and contain infected systems, while threat intelligence solutions keep the key personnel informed about evolving threats.

Table 7 presents the results of the third FMEA analysis, where formal, documented, and enforced change management controls are necessary to ensure system integrity. Similar measures are needed to establish secure system functionalities supporting sales campaigns.

Change management involves formal requests and approvals, testing and validating changes, and conducting post-implementation reviews to identify any underlying issues or security vulnerabilities. Additionally, controls such as automated monitoring tools and performance metrics can be used to detect deviations from these processes, whereas staff training and awareness are among

Table 7. FMEA for change management control.

ID	Potential failure mode	Potential effects of failure	Potential causes	Typical prevention controls	Typical detection controls
3.	The company's change management controls are maintained to ensure information security				
3.1	Insufficient change management measures in information systems	• The loss of system integrity and data confidentiality in systems and customer portals leads to legal liabilities and reputational damage • The loss of system integrity and potential for illegal exploitation of sales campaign features leads to financial losses	• Shortcomings in secure system development processes • Shortcomings in change management processes	• Change request and approval process • Testing and validation process • Post- implementation review process • Change management audits • Security awareness training for key personnel	• Performance metrics and KPIs • Automated monitoring tools • Change management audits • Security awareness training for key personnel

Table 8. FMEA for access control management.

ID	Potential failure mode	Potential effects of failure	Potential causes	Typical prevention controls	Typical detection controls
4	The company's access controls are managed to ensure information security				
4.1	Shortcomings in access controls management	• Malicious or unauthorized access to information • Insufficient tracing of user actions • Theft of information and other harmful actions lead to further cascading effects such as legal, reputational, operational, and financial damages	• Shortcomings in policy implementation • Lack of instructions • Lack of training and awareness • Technological limitations	• Access control policy and instructions • Strong authentication • Centralized identity and access management solution • Access logging • Security awareness training for key personnel	• Automated monitoring and alerting with user behavior analytics • Compliance audits and access reviews • Security awareness training for key personnel

the most important controls in ensuring the instructions are followed.

Therefore, energy retail companies should establish and enforce rules to ensure a secure software and system development lifecycle. This process should also include establishing risk-based security requirements and fully documenting procedures for all phases of system acquisition (ISO/IEC 27002: 2022).

Table 8 presents the results of the fourth FMEA analysis. Access control management stands among the top critical areas of information security, preventing malicious and unauthorized access to information (ISO/IEC 27002: 2022). Therefore, an access controls policy with clear implementation instructions, supported by staff awareness and training, is necessary to ensure only authorized and recorded access to systems and information. Software solutions for identity and access management allow for the centralized management of system-based access controls. This ensures the administration of role-based, least privileged, and segregated access to information while generating automated log files and audit trails.

Furthermore, strong authentication, requiring users to provide two or more forms of verification before accessing a system or resource, significantly improves security (ISO/IEC 27002: 2022). Compliance audits and access reviews help identify process shortcomings and discrepancies in user rights, while user behavior analytics can automatically monitor and highlight suspicious activities.

Table 9 presents the results of the fifth FMEA analysis. Managing insider threats begins with risk assessment because, once the areas of possible insider attacks are evaluated, the position to defend is already improved (Prabhu & Thompson, 2021). A mitigation plan should include implementing access controls to prevent unauthorized access, while Data Loss Prevention (DLP) solutions can be used to monitor sensitive data and control its transfer between endpoints. Relevant sensitive data should be encrypted both in transit and at rest to protect it from illegal access or interception (ISO/IEC 27002: 2022). Network segmentation reduces the attack surface and can isolate critical assets, limiting the potential for lateral movement by malicious insiders within the network.

Table 9. FMEA for insider threat recognition and control.

ID	Potential failure mode	Potential effects of failure	Potential causes	Typical prevention controls	Typical detection controls
5.	The company recognizes and controls potential insider threats				
5.1	The potential insider threat is not taken into account and further mitigated	• Compromised accounts and unauthorized access • Loss of confidentiality of sensitive information or intellectual property • Installation of malware • Social engineering • Execution of financial scams	• The insider threat is not included in the company's cyber risk management strategy • Insiders with malicious intent	• Insider risk assessment • Access control management • Data loss prevention (DLP) solution • Encryption of sensitive data and communications • Network segmentation • Vetting and background screenings for new employees • Onboarding and offboarding processes	• Data loss prevention (DLP) solution • User and entity behavior analytics (UEBA) • Whistleblowing process for reporting misconduct

Table 10. FMEA for data protection compliance.

ID	Potential failure mode	Potential effects of failure	Potential causes	Typical prevention controls	Typical detection controls
6.	The company ensures data protection compliance to protect customers' personal information				
6.1	Shortcomings in adhering adequately to data protection laws	• Processing customer personal data without legal grounds can lead to legal consequences, loss of customer trust, reputational damage, competitive disadvantage, and financial loss	• Shortcomings and a lack of clear roles and responsibilities in sales and customer service processes • Incomplete instructions • Lack of training and awareness	• Implementation of privacy information management system (PIMS) • Instructions for process responsibilities • Maintenance of up-to-date, data privacy-compliant sales processes overseen by the responsible personnel • Staff training and awareness	• Analysis of data breach reports • Compliance and process auditing
6.2	Shortcomings in the customer contract management process	• Loss of information confidentiality in the customer contract management process can lead to legal consequences, loss of customer trust, reputational damage, competitive disadvantage, and financial loss	• Immature processes in customer contract management • Lack of training and awareness	• Optimization of the customer contract management process • Staff training and awareness	• Analysis of data breach reports • Key performance indicators (KPIs) • Compliance and process auditing
6.3	Shortcomings in adhering adequately to secure electronic data handling instructions	• Noncompliant handling and storage of customers' data • Loss of customer data confidentiality can lead to legal consequences, loss of customer trust, reputational damage, competitive disadvantage, and financial loss	• Insufficient training and awareness about secure data handling • Shortcomings in processes to ensure timely retention of information	• Implementation of privacy information management system (PIMS) • Training and awareness of instructions for transferring, using, and storing customer information • Maintenance of up-to-date, data privacy-compliant sales processes overseen by the responsible personnel	• Analysis of data breach reports • Compliance and process auditing

User and Entity Behavior Analytics (UEBA) can detect anomalies such as unauthorized access and large data downloads, which should automatically be flagged for further investigation. Before onboarding, employees should undergo background checks and vetting to verify candidates' legitimacy. Whistleblowing functions facilitate anonymous reporting and early threat detection, while offboarding processes ensure access revocation and secure closure for departed employees.

Table 10 presents the results of the sixth FMEA analysis regarding compliance with data protection laws. Systematic data protection can be achieved by implementing a Privacy Information Management System (PIMS), which is commonly associated with the principles and controls of the ISO/IEC 27701 standard (ISO/IEC 27701: 2019).

Up-to-date, documented sales processes, facilitated by their formal owners, instructions, training, and awareness, are key to ensuring adherence to data protection-compliant daily sales operations. Auditing and analyzing of internal data breach reports is essential for identifying areas for improvement.

Customer contract management processes should be optimized and monitored with key performance indicators to reduce errors. Additionally, awareness and training on how to transfer, use, and store customer information are necessary for adhering to secure electronic data handling practices (ISO/IEC 27701: 2019). Furthermore, timely data retention can only be ensured by maintaining up-to-date, documented sales processes, overseen by responsible personnel who own these processes.

Table 11. FMEA for supply chain resilience.

ID	Potential failure mode	Potential effects of failure	Potential causes	Typical prevention controls	Typical detection controls
7.	The company's supply chain adheres to the company's information security requirements				
7.1	Shortcomings in asset management implementation	• Not all systems are included in the formal system landscape • Systems are taken into use without adequate contractual requirements • Suppliers' cybersecurity risks are not fully controlled • Supplier data breaches could compromise information confidentiality, integrity, and availability, causing operational disruptions and financial and reputational harm	• Incomplete asset management process • Insufficient roles and responsibilities in asset management • Lack of training and awareness	• Enforced asset management policy • Asset management process with defined roles and responsibilities • Security awareness training for key personnel	• IT asset scanner • Asset management process audits • IT landscape audits

Table 11 presents the results of the seventh FMEA analysis. Energy retail companies should ensure that their suppliers adhere to business-relevant, risk-based contractual information security requirements (ISO/IEC 27002: 2022). An asset management policy should be enforced to ensure that all information systems, including both internally developed systems and those provided by external suppliers, are consistently included in the formal IT system register.

Establishing formal ownership of systems, suppliers, and contracts helps guarantee that cybersecurity requirements are consistently implemented and managed by designated owners in supplier contracts (ISO/IEC 27002: 2022). Training and awareness initiatives for key personnel should be carried out to integrate these processes into daily operations. Furthermore, asset management and the IT landscape should undergo periodic audits and continuous process optimization, while using an IT asset scanner helps identify shadow IT, thereby improving the accuracy of the asset inventory.

Table 12 presents the results of the eighth FMEA analysis concerning the physical dimension of cybersecurity in energy retail companies, where the safety and well-being of staff members are always the highest priority. Therefore, a zero-tolerance policy toward threatening situations should be established.

Additionally, training and awareness of conflict resolution, as well as guidance on when to involve security and law enforcement, should be provided to staff members. Surveillance cameras, alarm systems, and the presence of security personnel enhance safety, while incidents should always be analyzed, with corrective actions taken to prevent recurrence.

Damage to company property can be caused by attempted burglary, vandalism, sabotage, or theft; thus, it is important to harden the relevant physical entry points and apply controls such as lighting, video surveillance, and guards, as well as label the equipment with unique identifiers, such as Radio Frequency Identification (RFID) tags for tracking and identification.

Access to company premises must be strictly controlled to prevent unauthorized individuals from entering, stealing information and equipment, causing damage, or posing physical threats to employees. This can be accomplished by strengthening physical access controls and implementing risk-based processes to verify employees and visitors entering the workplace (ISO/IEC 27002: 2022). All employees should understand these procedures to prevent tailgating and unauthorized entry.

To prevent further damage from lost or stolen mobile devices, all company-provided devices should be included in the mobile device management (MDM) system. MDM enables remote tracking and wiping of lost or stolen devices, as well as device encryption and strong authentication. Employees should be reminded to stay vigilant about securing their devices to minimize the risk of devices being lost or stolen.

Finally, the clean desk policy should be known and followed by all members of staff to prevent the loss of confidential information and theft of data and devices. Visual inspections and audits ensure that clean desk instructions for secure storage and controlled destruction of physical information are followed.

Table 12. FMEA for physical security management.

ID	Potential failure mode	Potential effects of failure	Potential causes	Typical prevention controls	Typical detection controls
8.	The company manages physical security to ensure employee safety and information security				
8.1	Concerns about the safety and well-being of customer interface employees	• Employees subjected to aggression • Employee mental discomfort	• Threats towards customer interface employees and the company	• Zero tolerance policy towards threats and aggressive behavior • Training and awareness of conflict resolution • Instructions on when to involve security and law enforcement • Surveillance cameras, alarm systems, and security guards	• Incident reporting and analysis • Auditing of access, equipment, surveillance, locations, and storage
8.2	Damage to company property and equipment	• Damaged physical premises • Damaged or stolen equipment • Disruption of operations • Financial loss	• Attempted burglary • Vandalism • Sabotage • Theft	• Hardened physical entry points • Motion-activated lighting • Visible surveillance systems • Staff training and awareness • Security guards • Labeling of assets with traceable identifiers	• Incident reporting and analysis • Auditing access, equipment, surveillance, locations, and storage • Surveillance systems • Security guards
8.3	Insufficient measures to prevent illegitimate access to company premises	• Outsiders on company premises with potential malicious intent • Physical threats towards employees • Theft of information • Damage to property • Shortcomings in logging company visitors	• Inadequate physical access control implementation • Inadequate training and awareness	• Process of authenticating employees and visitors accessing the company premises • Staff training and awareness	• Incident analysis • Auditing access, equipment, surveillance, locations, and storage
8.4	Shortcomings in minimizing the risks of stolen or lost mobile devices	• Lost or stolen mobile devices • Unauthorized access and loss of information confidentiality • Spread of malware • Financial losses	• Human errors • Carelessness • Accidents • Theft • Shortcomings in training and awareness • Inadequate mobile device management controls	• Mobile device management for company-provided devices • Remote tracking and wiping of devices • Device encryption and strong authentication • Staff training and awareness	• Mobile device management for company-provided devices • Remote tracking and wiping of devices
8.5	Inadequate measures to implement clean desk practices	• Loss of confidentiality of sensitive information and intellectual property • Theft of equipment and information	• Human errors • Carelessness • Negligence • Shortcomings in training and awareness • Lack of monitoring	• Staff training and awareness • Secure storage and destruction of physical information • Automated screen locking • Visual inspections and audits	• Staff training and awareness • Visual inspections and audits

4.3. Graphical cyberattack visualization with the bowtie model

In this section, the bowtie model is used to visualize two types of cyberattacks. Figure 4 illustrates a phishing attack, adapted from Table 5, ID 1.1, and emphasizes the importance of user awareness as the primary defense against socially engineered phishing attacks.

In this example, the attacker's goal is to acquire the access credentials of privileged users and install malware on the users' devices. The attacker may initially use generic phishing via e-mail, which is caught by the defenders' spam filter. However, the attackers can use social engineering techniques to customize the phishing content, making it appear legitimate to bypass the spam filters and attract the target's attention.

The attackers may exploit insufficient awareness among privileged access users in order to acquire their user credentials. Therefore, the defense is to train these users and improve awareness through e-mail phishing simulations. However, in this scenario, to bypass these defenses, the attackers also conduct phishing through various other electronic communication channels, such as SMS, voice phishing, or instant messaging.

Defenders implement strong authentication for privileged accounts, requiring two or more authentication factors for access, thereby significantly improving security. Attackers may again employ various social engineering techniques to bypass these defensive measures, such as blackmailing their targets through fear and manipulation. However, the best protection against phishing is user awareness and a strong, positive security culture that encourages incident reporting.

If attackers succeed in acquiring the credentials, the detective control is a behavioral analytics solution, which restricts access based on specific geolocation and time. Attackers may attempt to bypass this control by timing their attacks and masking their IP addresses. Finally, endpoint security solutions prevent malware, forcing attackers to use more sophisticated methods to execute malicious files, which could lead to ransomware infection with cascading effects.

Another example visualizes unauthorized physical access, adapted from Table 12, ID 8.3. Figure 5 illustrates this attack, where an attacker attempts to tailgate or steal an employee ID badge to gain unauthorized access to company premises and steal physical storage media containing sensitive information. Tailgating is an attack by malicious outsiders without proper credentials by following closely behind an authorized company employee inside the company premises.

The possibility of this attack being successful is reduced by mandating employees to wear ID badges and by training staff to be vigilant and act if intruders are noticed. However, the tailgater may always try to impersonate a credible visitor. Tailgating is more difficult if the company premises are protected with ID access card readers, along with strong authentication methods such as

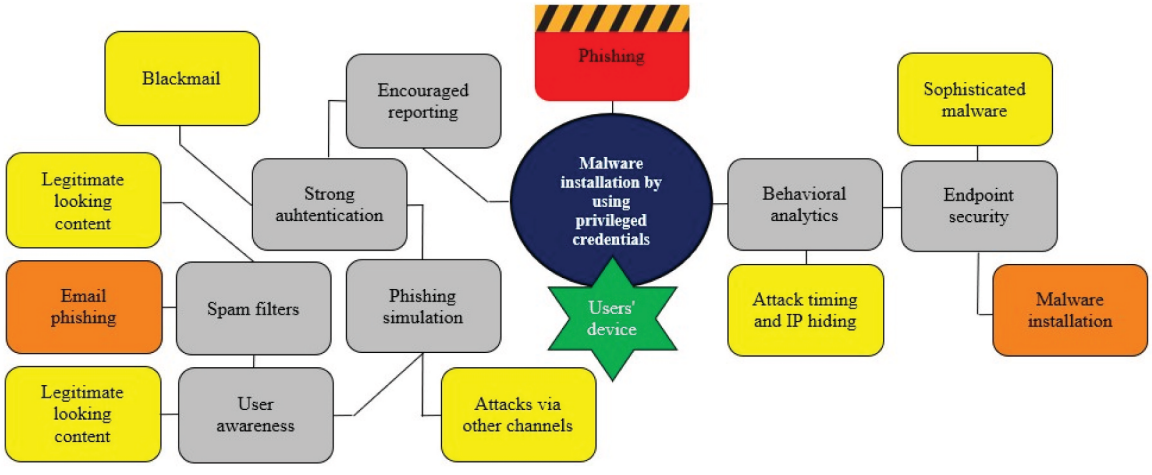

Figure 4. Phishing attack example visualized using a bowtie model.

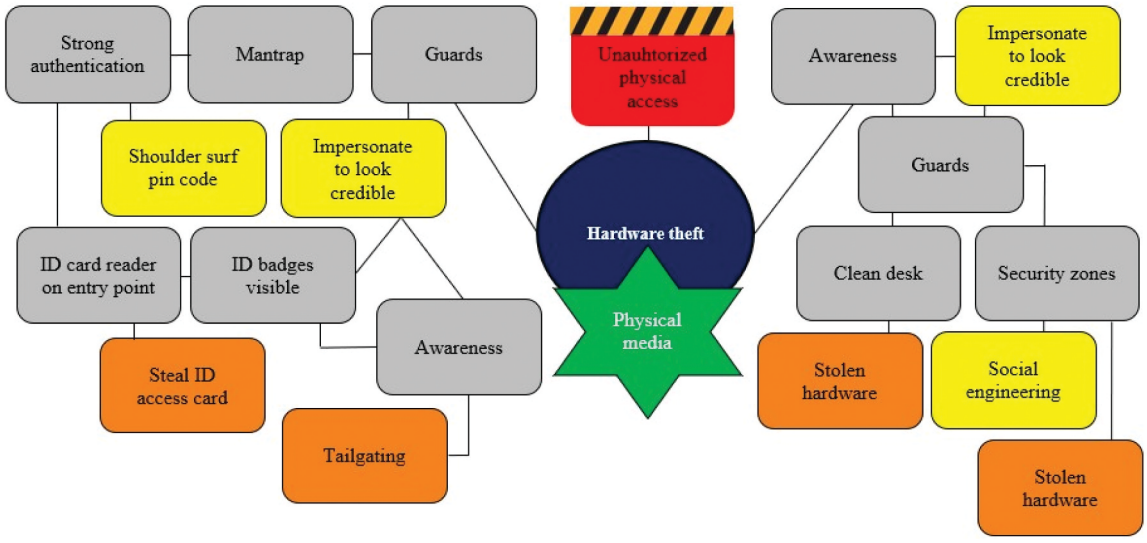

Figure 5. Unauthorized entry attack example visualized by bowtie model.

a PIN code reader at the entry point, while mantraps provide an additional layer of defense at entrances.

The attacker may also try to steal the authenticated user's access card, where strong authentication at entry points is again an important measure to prevent the attack from being successful. However, the attacker can attempt to shoulder surf the PIN code entry before stealing the access card. Therefore, employee vigilance and awareness are necessary protections, while guards and surveillance add additional defensive layers. If the attacker gains unauthorized access, vigilant employees, guards, and surveillance can still stop the attacker.

A clean desk policy, in which equipment and storage media are not left unattended reduces the likelihood of the attack being successful. Secure zones within company premises provide an added layer of protection, making it much harder for attackers to use social engineering techniques to bypass security.

5. Discussion

The analysis of cybersecurity incidents in the energy retail sector from 2018 to 2023 identifies eight key risk categories, each requiring tailored mitigation strategies. The Failure Modes and Effects Analysis (FMEA) offers a structured approach to addressing these risks, outlining common mitigation measures specific to the energy retail business to protect critical assets, ensure regulatory compliance, and avoid sanctions from authorities due to noncompliance with cybersecurity regulations.

To manage risks, energy retailers must proactively govern their information security management system (ISMS). A multi-layered approach combining technical defenses, organizational processes, and staff education is essential for protection against cyberattacks such as denial of service attacks, brute force attacks, and ransomware attacks, which present significant security challenges. Phishing attacks, which exploit social engineering to deceive users, can be mitigated through awareness training, simulated exercises, and multifactor authentication (MFA).

Formalized change management controls are necessary for energy companies to maintain system integrity and prevent data breaches. This includes documented procedures, monitoring tools, staff training, and risk-based security requirements throughout the system acquisition and development lifecycle.

Access management controls are equally important for energy retailers. Effective policies, staff training, identity management software, strong authentication, and detective controls such as audits and behavioral analytics are key measures for mitigating the risk of unauthorized access to information.

In energy retail companies, mitigating insider threats, whether malicious or negligent, always begins with comprehensive risk assessments, followed by security training, implementing access controls, and restricting access to sensitive information. Additionally, conducting thorough background checks and vetting of employees contributes to prevent potential risks from materializing.

Energy retail companies process large volumes of customer personal information, making data breaches and noncompliance more likely without proactive measures. A systematic approach, such as implementing a Privacy Information Management System (PIMS), can mitigate these risks. Awareness and training on secure data handling practices should be mandatory, while up-to-date sales processes must be managed by responsible personnel to ensure ownership and compliance. Additionally, optimizing customer contract management with key performance indicators reduces errors.

Energy retailers must ensure that their suppliers adhere to risk-based information security requirements. Enforcing an asset management policy with formal ownership and periodic audits will optimize processes, identify shadow IT, and improve the accuracy of asset inventories, including registers of information systems, contracts, and key processes.

Energy retail companies also face serious physical cybersecurity risks, which must be managed through access control, surveillance, and secure asset disposal to prevent unauthorized access, theft, and data breaches. These measures are necessary for preventing potential harm to personnel, ensuring uninterrupted operations, and maintaining business continuity.

Shortcoming of the risk categories and FMEA framework presented, is that they do not capture the interplay between different risks and attack-defense patterns. For example, a ransomware attack often begins with phishing, highlighting the need for models that visualize these interconnected threats. The Bowtie model was demonstrated earlier through two distinct examples. The first example illustrated malware installation on a user's device via socially engineered phishing, exploiting privileged access credentials, while the second depicted stolen hardware resulting from unauthorized entry into an organization's premises through tailgating and theft of an employee's ID access card.

The Bowtie model complements risk categorization and FMEA by providing a visual representation of risk pathways, illustrating how multiple risks can interconnect. Bowties enhance understanding by mapping both attacks and defensive measures, providing a layered and more comprehensive approach to managing complex cybersecurity risks and incidents.

6. Conclusions

This section presents the conclusions of the study, including its theoretical and practical contributions, as well as its limitations and suggestions for future research.

6.1. Theoretical contributions

A notable gap exists in the literature regarding the cybersecurity risk management for energy retail companies. Consequently, energy retailers face increased legal pressure to manage cybersecurity risks and protect critical infrastructures (Haber & Zarsky, 2018), while they remain a prime target for cybercriminals due to their financial value within the energy industry value chain (Dagoumas, 2019).

From a theoretical perspective, this work builds on the study by Soomro et al. (2016) by detailing cybersecurity risks in the energy retail sector and contributes to the future research agenda of Patterson et al. (2023) on learning from cybersecurity incidents. The work also reflects the research of Staheli et al. (2014) and de Ruijter and Guldenmund (2016) by demonstrating how graphical cyberattack visualizations using the Bowtie model can enhance the understanding of these risks in the energy retail sector. By integrating these perspectives, this work provides a more resilient framework for mitigating cybersecurity risks in this critical industry sector.

6.2. Practical contributions

This study identifies eight distinct cybersecurity risk categories faced by energy retail businesses, offering detailed insights into failure modes and risk management strategies. By incorporating these categories and strategies into their risk assessment and management processes, energy retail companies and organizations managing critical infrastructure can better align with new cybersecurity laws, such as the NIS 2 Directive, which mandates the protection of critical infrastructures and requires management oversight of risk management practices.

The Bowtie analysis complements these efforts by providing a clear visual representation of interrelated cybersecurity risks and controls, helping management understand potential threats and ensure compliance with NIS 2 Directive obligations. By mapping both preventative and mitigative controls, the Bowtie method enhances risk communication across the organization, making it easier for stakeholders to grasp complex risk scenarios and take informed decisions to address vulnerabilities.

However, organizations may face implementation challenges, including the need for management support, financial constraints, and resource allocation, particularly in the context of change management, organizational culture, and leadership commitment (Vincent et al., 2018). Other barriers include resistance to policy changes, employee motivation issues, gaps in awareness and skills, and difficulties in fostering collaboration across departments (Uchendu et al., 2021).

6.3. Limitations and future directions

This study has three notable limitations. First, as a single case study, it may not fully capture the broader landscape of cybersecurity risks among energy retailers and critical infrastructure businesses. The findings are based on a single energy retail organization, whose cybersecurity risk posture is influenced by specific factors such as organizational culture, regulatory requirements, leadership style, and resource allocation. Since these factors vary across organizations and industry sectors, the findings have limited generalizability. This underscores the need for future research to examine cybersecurity risks and defense strategies more comprehensively, using comparative case studies or cross-sector analyses to gain deeper insights.

The second limitation is the temporal scope, focusing on cybersecurity incidents reported between 2018 and 2023. Given the fast evolving nature of cyber security attack vectors and risks, future changes in trends and technologies, along with their corresponding countermeasures, may not be reflected in the results of this study. A longitudinal approach in future research could identify emerging technology patterns and new attack-defense vectors.

The third limitation concerns the prevention and detection controls outlined in the FMEA analysis, which represent typical measures that energy retail companies can implement. In practice, each company may apply different controls based on their specific business risks. Furthermore, the reliance of the FMEA on subjective and qualitative assessments may lead to variations among practitioners, resulting in different outcomes.

Despite these limitations, this study addresses a significant research gap in the critical energy retail sector. Future studies are encouraged to provide more incident-based evidence on cybersecurity risks and mitigation strategies for managing the IT-GRC of energy retail companies. Subsequent research efforts should also focus on standardizing the visualization of cybersecurity risks for executive management teams. This would improve their understanding of attack patterns and support the implementation of effective defense strategies.

Acknowledgments

Generative AI tools, specifically ChatGPT (version GPT-4), were used for language improvement purposes in this manuscript.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Mikko Suorsa http://orcid.org/0000-0002-1649-4223
P. Helo http://orcid.org/0000-0002-0501-2727

References

Abdo, H., Kaouk, M., Flaus, J., & Masse, F. (2017). Towards a better industrial risk analysis: A new approach that combines cybersecurity within safety. In *Proceedings of the 27th European Safety and Reliability Annual Conference (ESREL 2017)*, Porto, Portugal (pp. 1215–1222).

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process. *Institute of Electrical and Electronics Engineers Access*, 1–1. https://doi.org/10.1109/ACCESS.2021.3066383

Akula, S. K., & Salehfar, H. (2021). Risk-based classical failure mode and effect analysis (FMEA) of microgrid cyber-physical energy systems. *North American Power Symposium, NAPS*, 1–6. https://doi.org/10.1109/NAPS52732.2021.9654717

Al-Mhiqani, M., Rabiah, A., Zaheera, Z. A., Warusia, M., Aslinda, H., & Clarke, N. (2018). A new taxonomy of insider threats: An initial step in understanding authorized attack. *International Journal of Information Systems and Management*, *1*(4), 343–359. https://doi.org/10.1504/IJISAM.2018.10014439

Almudaires, F., & Almaiah, M. (2021). Data an overview of cybersecurity threats on credit card companies and credit card risk mitigation. In *2021 International Conference on Information Technology (ICIT)* (pp. 732–738). IEEE. https://doi.org/10.1109/ICIT52682.2021.9491114

Ang, C. K. G., & Utomo, N. P. (2017). Cyber security in the energy world. In *2017 Asian Conference on Energy, Power and Transportation Electrification (ACEPT)* (pp. 1–5). https://doi.org/10.1109/ACEPT.2017.8168583

Ani, U. P. D., He, H., & Tiwari, A. (2016). Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. *Journal of Cyber Security Technology*, *1*(1), 32–74. https://doi.org/10.1080/23742917.2016.1252211

Asllani, A., Lari, A., & Lari, N. (2018). Strengthening information technology security through the failure modes and effects analysis approach. *International Journal of Quality Innovation*, *4*(5). https://doi.org/10.1186/s40887-018-0025-1

Azzuni, A., & Breyer, C. (2017). Definitions and dimensions of energy security: A literature review. *WIREs Energy and Environment*, *7*(1). https://doi.org/10.1002/wene.268

Babeshko, I., & Giandomenico, F. D. (2023). Safety and cybersecurity assessment techniques for critical industries: A mapping study. *Institute of Electrical and Electronics Engineers Access*, *11*, 83781–83793. https://doi.org/10.1109/ACCESS.2023.3297446

Barichella, A. (2023). Cybersecurity and data protection in the power sector: Challenges, perspectives, and policy approaches. In J. I. Considine, S. Cote, D. Cooke, & G. Wood (Eds.), *A research agenda for energy politics* (pp. 233–260). Edward Elgar Publishing. https://doi.org/10.4337/9781789901764.00022

Bederna, Z., & Rajnai, Z. (2022). Analysis of the cybersecurity ecosystem in the European Union. *International Cybersecurity Law Review*, *3*(1), 35–49. https://doi.org/10.1365/s43439-022-00048-9

Bernsmed, K., Frøystad, C., Meland, P. H., Nesheim, D. A., & Rødseth, Ø. J. (2018). Visualizing cyber security risks with bow-tie diagrams. In P. Liu, S. Mauw, & K. Stolen (Eds.), *Graphical models for security. GraMSec 2017. Lecture notes in computer science* (Vol. 10744, pp. 43–60). Springer. https://doi.org/10.1007/978-3-319-74860-3_3

Bıçakcı, A. S., & Evren, A. G. (2022). Thinking multiculturality in the age of hybrid threats: Converging cyber and physical security in Akkuyu nuclear power plant. *Nuclear Engineering and Technology*, *54*(7), 2467–2474. https://doi.org/10.1016/j.net.2022.01.033

Brereton, P., Kitchenham, B., Budgen, D., & Li, Z. (2008). Using a protocol template for case study planning. In *12th International Conference on Evaluation and Assessment in Software Engineering (EASE)* (pp. 1–8). https://doi.org/10.14236/ewic/EASE2008.5

Brown, M., Woodhouse, S., & Sioshansi, F. (2019). Digitalization of energy. In F. Sioshansi (Ed.), *Consumer, prosumer, Prosumager: How service innovations will disrupt the utility business Model* (pp. 3–25). Academic Press.

Calandro, E. (2020). Observing global cyber norms nationally - the case of critical infrastructure protection in South Africa. *SSRN*. https://doi.org/10.2139/ssrn.3895156

Calder, A., & Gerard, L. (2013). The ISO/IEC 27001 family of information security standards. In *ISO 27001/ISO 27002, a pocket guide* (pp. 12–14). IT Governance Ltd.

Carlson, C. S. (2012). *Effective FMEAs: Achieving safe, reliable, and economical products and processes using failure mode and effects analysis*. John Wiley & Sons, Inc. https://doi.org/10.1002/9781118312575

Chen, Z., Guo, Y., Bai, D., Wang, J., Dong, Y., Qian, S., Lu, T., & Xing, H. (2021). Research on cyber security defense and protection in the power industry. *Journal of Physics: Conference Series*, *1769*(1), 012040. https://doi.org/10.1088/1742-6596/1769/1/012040

Chevreau, F. R., Wybo, J. L., & Cauchois, D. (2006). Organizing learning processes on risks by using the bow-tie representation. *Journal of Hazardous Materials*, *130*(3), 276–283. https://doi.org/10.1016/j.jhazmat.2005.07.018

Chiara, P. G. (2022). Das Cyberresilienzgesetz – Vorschlag der Europäischen Kommission für eine horizontale Verordnung zur Cybersicherheit für Produkte mit digitalen Komponenten. *International Cybersecurity Law Review*, *3*(2), 255–272. https://doi.org/10.1365/s43439-022-00067-6

Cormier, A., & Ng, C. (2020). Integrating cybersecurity in hazard and risk analyses. *Journal of Loss Prevention in the Process Industries*, *64*, 104044. https://doi.org/10.1016/j.jlp.2020.104044

Dagoumas, A. (2019). Assessing the impact of cybersecurity attacks on power systems. *Energies*, *12*(4), 725. https://doi.org/10.3390/en12040725

de Ruijter, A., & Guldenmund, F. (2016). The bowtie method: A review. *Safety Science*, *88*, 211–218. https://doi.org/10.1016/j.ssci.2016.03.001

Dogan, B., & Edwards, K. (2022). Impact of ransomware attacks on enterprises within the retail industry. [Unpublished research proposal]. https://doi.org/10.13140/RG.2.2.29008.17928/1

Dolezilek, D., & Hussey, L. (2011). Requirements or recommendations? Sorting out NERC CIP, NIST, and DOE cybersecurity. In 2011 *64th Annual Conference for Protective Relay Engineers* (pp. 328–333). https://doi.org/10.1109/CPRE.2011.6035634

Dooley, L. M. (2002). Case study research and theory building. *Advances in Developing Human Resources*, *4*(3), 335–354. https://doi.org/10.1177/1523422302043007

Dragomir, A. V. (2021). What's new in the NIS 2 directive proposal compared to the old NIS directive. *SEA-Practical Application of Science*, *9*(27), 155–162.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review*, *14*(4), 532–550.

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal*, *50*(1), 25–32. https://doi.org/10.5465/amj.2007.24160888

Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research*, *272*(3), 1109–1119. https://doi.org/10.1016/j.ejor.2018.07.021

European Commission. (2020). *Joint communication to the European parliament and the council: The EU's cybersecurity strategy for the digital decade (document 52020JC0018)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0018

European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*. https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Union. (2016). Directive (EU) 2016/1148 of the European parliament and of the council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the union (NIS directive). *Official journal of the European Union, L 194*. (1–30). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148

European Union. (2022). Directive (EU) 2022/2555 of the European parliament and of the council of 14 December 2022 on measures for a high common level of cybersecurity across the union, amending regulation (EU) No 910/2014 and directive (EU) 2018/1972, and repealing directive (EU) 2016/1148 (NIS 2 directive). *Official journal of the European Union, L 333*. (80–119). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

Faheem, M., Shah, S. B. H., Butt, R. A., Raza, B., Anwar, M., Ashraf, M. W., Ngadi, M. A., & Gungor, V. C. (2018). Smart grid communication and information technologies in the perspective of industry 4.0: Opportunities and challenges. *Computer Science Review*, *30*, 1–30. https://doi.org/10.1016/j.cosrev.2018.08.001

Falowo, O. I., Popoola, S., Riep, J., Adewopo, V. A., & Koch, J. (2022). Threat actors' tenacity to disrupt: Examination of major cybersecurity incidents. *Institute of Electrical and Electronics Engineers Access*, *10*, 134038–134051. https://doi.org/10.1109/ACCESS.2022.3231847

Garfinkel, S. L. (2015). *De-identification of personal information (NISTIR 8053)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.IR.8053

Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., Doukas, G., Kontoulis, M., Nikoloudakis, Y., Marin, S., Cabecinha, R., & Ntanos, C. (2022). A cybersecurity culture survey targeting healthcare critical infrastructures. *Healthcare*, *10*(2), 327. https://doi.org/10.3390/healthcare10020327

Gong, S., & Lee, C. (2021). Cyber threat intelligence framework for incident response in an energy cloud platform. *Electronics*, *10*(3), 239. https://doi.org/10.3390/electronics10030239

Gouglidis, A., Green, B., Hutchison, D., Alshawish, A., & de Meer, H. (2018). Surveillance and security: Protecting electricity utilities and other critical infrastructures. *Energy Informatics*, *1*(15). https://doi.org/10.1186/s42162-018-0019-1

Govea, J., Gaibor-Naranjo, W., & Villegas-Ch, W. (2024). Transforming cybersecurity into critical energy infrastructure: A study on the effectiveness of artificial intelligence. *Systems*, *12*(5), 165. https://doi.org/10.3390/systems12050165

Haber, E., & Zarsky, T. (2018). Cybersecurity for infrastructure: A critical analysis. *Florida State University Law Review*, *44*(2).

Hamdare, S., Kaiwartya, O., Aljaidi, M., Jugran, M., Cao, Y., Kumar, S., Mahmud, M., Brown, D., & Lloret, J. (2023). Cybersecurity risk analysis of electric vehicle charging stations. *Sensors (Switzerland)*, *23*(15), 6716. https://doi.org/10.3390/s23156716

Hancock, D. R., Algozzine, B., & Lim, J. H. (2021). *Doing case study research: A practical guide for beginning researchers*. Teachers College Press.

Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, M. K. (2020). A review of cybersecurity incidents in the water sector. *Journal of Environmental Engineering*, *146*(5), 1–13. https://doi.org/10.1061/(ASCE)EE.1943-7870.0001686

Hseiki, H., El Hajj, A., Ajra, Y., Hija, F., & Haidar, A. (2024). A secure and resilient smart energy meter. *Institute of Electrical and Electronics Engineers Access*, *12*, 3114–3125. https://doi.org/10.1109/ACCESS.2023.3349091

ISO/IEC 27001: 2022. (2022). *Information technology - security techniques - information security management systems - requirements*. International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

ISO/IEC 27002: 2022. (2022). *Information security, cybersecurity and privacy protection - information security controls*. International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

ISO/IEC 27701: 2019. (2019). *Security techniques - extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - requirements and guidelines*. International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

ISO/IEC 61025: 2006. (2006). *Fault tree analysis (FTA)*. International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

Ji, X., Yu, H., Fan, G., & Fu, W. (2016). Attack-defense trees based cyber security analysis for CPSs. In *17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)* (pp. 693–698). https://doi.org/10.1109/SNPD.2016.7515980

Kordy, B., Mauw, S., Melissen, M., & Schweitzer, P. (2010). Attack-defense trees and two-player binary zero-sum extensive form games are equivalent. In T. Alpcan, L. Buttyán, & J. S. Baras (Eds.), *Decision and game theory for security (GameSec 2010)* (p. 6442). https://doi.org/10.1007/978-3-642-17197-0_17

Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021). Cybersecurity in power grids: Challenges and opportunities. *Sensors (Switzerland)*, *21*(18), 6225. https://doi.org/10.3390/s21186225

Kulkarni, A., Wang, Y., Gopinath, M., Sobien, D., Rahman, A., & Batarseh, F. A. (2024). A review of cybersecurity incidents in the food and agriculture sector [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2403.08036

Lallie, H. S., Debattista, K., & Bal, J. (2020). A review of attack graph and attack tree visual syntax in cyber security. *Computer Science Review*, *35*, 100219. https://doi.org/10.1016/j.cosrev.2019.100219

Lazar, J., Feng, J. H., & Hochheiser, H. (2017). Case studies. In J. Lazar, J. H. Feng, & H. Hochheiser (Eds.), *Research methods in human-computer interaction* (pp. 153–184). Morgan Kaufmann Publishers.

Lee, J. H., Shin, J., & Seo, J. T. (2023). Solar power plant network packet-based anomaly detection system for cybersecurity. *Computers, Materials & Continua*, *77*(1), 757–779. https://doi.org/10.32604/cmc.2023.039461

Lewis, S., & Smith, K. (2010). Lessons learned from real world application of the bow-tie method. In *Proceedings of the 6th Global Congress on Process Safety*, San Antonio, Texas, USA (pp. 22–24).

Line, M. B., Tøndel, I. A., & Jaatun, M. G. (2014). Information security incident management: Planning for failure. In *Eighth International Conference on IT Security Incident Management & IT Forensics* (pp. 47–61). https://doi.org/10.1109/IMF.2014.10

Löschel, A., Moslener, U., & Rübbelke, D. T. G. (2010). Energy security - concepts and indicators. *Energy Policy*, *38*(4), 1607–1608. https://doi.org/10.1016/j.enpol.2009.03.019

Markowski, A. S., & Kotynia, A. (2011). "Bow-tie" model in layer of protection analysis. *Process Safety and Environmental Protection*, *89*(4), 205–213. https://doi.org/10.1016/j.psep.2011.04.005

Maschmeyer, L., Deibert, R. J., & Lindsay, J. R. (2020). A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society. *Journal of Information Technology & Politics*, *18*(1), 1–20. https://doi.org/10.1080/19331681.2020.1776658

Melaku, H. M. (2023). A dynamic and adaptive cybersecurity governance framework. *Journal of Cybersecurity and Privacy*, *3*(3), 327–350. https://doi.org/10.3390/jcp3030017

Meland, P. H., Bernsmed, K., Frøystad, C., Li, J., & Sindre, G. (2019). An experimental evaluation of bow-tie analysis for security. *Information and Computer Security*, *27*(4), 536–561. https://doi.org/10.1108/ICS-11-2018-0132

Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., & Friday, D. (2021). New challenges in supply chain management: Cybersecurity across the supply chain. *International Journal of Production Research*, *60*(1), 162–183. https://doi.org/10.1080/00207543.2021.1984606

Mizrak, F. (2023). Integrating cybersecurity risk management into strategic management: A comprehensive literature review. *Pressacademia*, *3*, 98–108. https://doi.org/10.17261/Pressacademia.2023.1807

Moody, D. (2007). What makes a good diagram? Improving the cognitive effectiveness of diagrams in IS development. In W. Wojtkowski, W. G. Wojtkowski, J. Zupancic, G. Magyar, & G. Knapp (Eds.), *Advances in information systems development*. Springer. https://doi.org/10.1007/978-0-387-70802-7_40

Nagaraju, V., Fiondella, L., & Wandji, T. (2017). A survey of fault and attack tree modeling and analysis for cyber risk management. In *2017 IEEE International Symposium on Technologies for Homeland Security* (pp. 1–6). https://doi.org/10.1109/THS.2017.7943455

National Institute of Standards and Technology. (2024). *Cybersecurity framework 2.0 (NIST CSF 2.0)*. U.S. Department of Commerce. https://www.nist.gov/cyberframework

Nazari, Z., & Musilek, P. (2023). Impact of digital transformation on the energy sector: A review. *Algorithms*, *16*(4), 211. https://doi.org/10.3390/a16040211

Nikolaou, N., Papadakis, A., Psychogyios, K., & Zahariadis, T. (2023). Vulnerability identification and assessment for critical infrastructures in the energy sector. *Electronics*, *12*(14), 3185. https://doi.org/10.3390/electronics12143185

NIST SP 800-82r3. (2023). NIST special publication. Guide to operational technology (OT). *Security*. https://doi.org/10.6028/NIST.SP.800-82r3

Onwubiko, C., & Ouazzane, K. (2022). SOTER: A playbook for cybersecurity incident management. *IEEE Transactions on Engineering Management*, *69*(6), 3771–3791. https://doi.org/10.1109/TEM.2020.2979832

Osden, J., & Lubbe, S. (2009). Using information technology governance, risk (GRC) as a creator of business values - a case study. *South African Journal of Economic and*

Management Sciences, *12*(1), 115–125. https://doi.org/10.4102/sajems.v12i1.264

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the bitcoin ecosystem. *Journal of Cybersecurity*, *5*(1), 1. https://doi.org/10.1093/cybsec/tyz003

Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security*, *132*, 103309. https://doi.org/10.1016/j.cose.2023.103309

Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2024). "I don't think we're there yet": The practices and challenges of organisational learning from cyber security incidents. *Computers & Security*, *139*, 103699. https://doi.org/10.1016/j.cose.2023.103699

Pourmirza, Z., & Walker, S. (2021). Electric vehicle charging station: Cyber security challenges and perspective. In *IEEE 9th International Conference on Smart Energy Grid Engineering (SEGE)* (pp. 111–116). https://doi.org/10.1109/SEGE52446.2021.9535052

Prabhu, S., & Thompson, N. (2021). A primer on insider threats in cybersecurity. *Information Security Journal: A Global Perspective*, *31*(5), 602–611. https://doi.org/10.1080/19393555.2021.1971802

Rajkumar, V., Ştefanov, A., Presekal, A., Palensky, P., & Torres, J. (2023). Cyber attacks on power grids: Causes and propagation of cascading failures. *Institute of Electrical and Electronics Engineers Access*. https://doi.org/10.1109/ACCESS.2023.3317695

Schmitz-Berndt, S. (2023). Defining the reporting threshold for a cybersecurity incident under the NIS directive and the NIS 2 directive. *Journal of Cybersecurity*, *9*(1). https://doi.org/10.1093/cybsec/tyad009

SektorCERT. (2022, September). *Attacks against European energy and utility companies*. https://sektorcert.dk/wp-content/uploads/2022/09/Attacks-against-European-energy-and-utility-companies-2020-09-05-v3.pdf

Shah, R. (2023). *Getting regulation right, approaches to improving Australia's cybersecurity*. Policy brief report No. 73/2023. ASPI, Australian Strategic Policy Institute.

Sharma, K. D., & Srivastava, S. (2018). Failure mode and effect analysis (FMEA) implementation: A literature review. *Journal of Advance Research in Aeronautics and Space Science*, *5*(1 & amp;2), 1–17.

Shoetan, A., Okafor, A., Amoo, O., Okafor, E., Olorunfemi, O., & Shoetan, P. (2024). Synthesizing AI's impact on cybersecurity in telecommunications: A conceptual framework. *Computer Science & IT Research Journal*, *5*(3), 594–605. https://doi.org/10.51594/csitrj.v5i3.908

Skias, D., Tsekeridou, S., Zahariadis, T., Voulkidis, A., & Velivassaki, T. (2022). Demonstration of alignment of the Pan-European cybersecurity incidents information sharing platform to cybersecurity policy, regulatory and legislative advancements. In *Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22)* (Vol. 75, pp. 1–8). https://doi.org/10.1145/3538969.3544477

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Staheli, D., Yu, T., Crouser, R. J., Damodaran, S., Nam, K., O'Gwynn, D., McKenna, S., & Harrison, L. (2014). Visualization evaluation for cyber security: Trends and future directions. *Proceedings of the Eleventh Workshop on Visualization for Cyber Security* (*VizSec '14*), 49–56. https://doi.org/10.1145/2671491.2671492

Stewart, J. M., Chapple, M., & Gibson, D. (2012). *CISSP: Certified information systems security professional study Guide*. John Wiley & Sons, Inc.

Subriadi, A. P., & Najwa, N. F. (2020). The consistency analysis of failure mode and effect analysis (FMEA) in information technology risk assessment. *Heliyon*, *6*(1), e03161. https://doi.org/10.1016/j.heliyon.2020.e03161

Sun, C., Cardenas, D. S., Hahn, A., & Liu, C. (2020). Intrusion detection for cybersecurity of smart meters. In *IEEE Transactions on Smart Grid*. https://doi.org/10.1109/TSG.2020.3010230

Sun, C., Hahn, A., & Liu, C. (2018). Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, *99*, 45–56. https://doi.org/10.1016/j.ijepes.2017.12.020

Suorsa, M., & Helo, P. (2023). Information security failures identified and measured - ISO/IEC 27001: 2013 controls ranked based on GDPR penalty case analysis. *Information Security Journal: A Global Perspective*, *33*(3), 285–306. https://doi.org/10.1080/19393555.2023.2270984

Tøndel, I. A., Vefsnmo, H., Gjerde, O., Johannessen, F., & Frøystad, C. (2020). Hunting dependencies: Using bow-tie for combined analysis of power and cyber security. In *2nd International Conference on Societal Automation (SA)* (pp. 1–8). https://doi.org/10.1109/SA51175.2021.9507185

Tufail, S., Parvez, I., Batool, S., & Sarwat, A. (2021). A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid. *Energies*, *14*(18), 5894. https://doi.org/10.3390/en14185894

Tuptuk, N., Hazell, P., Watson, J., & Hailes, S. (2021). A systematic review of the state of cyber-security in water systems. *Water*, *13*(1), 81. https://doi.org/10.3390/w13010081

Tuyen, N. D., Quan, N., Linh, V., Tuyen, V., & Fujita, G. (2022). A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy. *Institute of Electrical and Electronics Engineers Access*, *10*, 1–1. https://doi.org/10.1109/ACCESS.2022.3163551

Uchendu, B., Jason, R. C., Nurse, M. B., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer*

Law & Security Review, *52*, 105890. https://doi.org/10.1016/j.clsr.2023.105890

Venkatachary, S., Prasad, J., & Samikannu, R. (2017). Economic impacts of cyber security in energy sector: A review. *International Journal of Energy Economics & Policy*, *7*(5), 250–262.

Vincent, N., Higgs, J., & Pinsker, R. (2018). Board and management-level factors affecting the maturity of it risk management practices. *Journal of Information Systems*, *33*, 10–30. https://doi.org/10.2308/isys-52229

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security - what goes where? *Information and Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wang, W., & Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. *Computer Networks*, *57*(5), 1344–1371. https://doi.org/10.1016/j.comnet.2012.12.017

Wen, H., & Faisal, K. (2023). Cybersecurity and process safety synergy: An analytical exploration of cyberattack-induced incidents. *The Canadian Journal of Chemical Engineering*, 1–12. https://doi.org/10.1002/cjce.25119

Whitehead, D. E., Owens, K., Gammel, D., & Smith, J. (2017). Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. In *70th Annual Conference for Protective Relay Engineers (CPRE)* (pp. 1–8). https://doi.org/10.1109/CPRE.2017.8090056

Wright, C. (2019). Cyber security governance. In C. Wright (Ed.), *How cyber security can protect your business: A guide for all stakeholders* (pp. 21–29). IT Governance Ltd.

Yin, R. K. (1994). Conducting case studies: Preparing for data collection. In R. K. Yin (Ed.), *Case study research: Design and methods* (pp. 57–81). Sage Publications.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Sage Publications.

Yusta, J. M., Correa, G. J., & Lacal-Arántegui, R. (2011). Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy Policy*, *39*(10), 6100–6119. https://doi.org/10.1016/j.enpol.2011.07.010

Zarreh, A., Wan, H., Lee, Y., Saygin, C., & Al Janahi, R. (2019). Risk assessment for cyber security of manufacturing systems: A game theory approach. *Procedia Manufacturing*, *38*, 605–612. https://doi.org/10.1016/j.promfg.2020.01.077

Zhang, F., & Kelly, K. (2022). Overview and recommendations for cyber risk assessment in nuclear power plants. *Nuclear Technology*, *209*(3), 488–502. https://doi.org/10.1080/00295450.2022.2092356

Zhang, Y., Xiang, Y., & Wang, L. (2016). Power system reliability assessment incorporating cyber attacks against wind farm energy management systems. *IEEE Transactions on Smart Grid*, *8*(5), 1–15. https://doi.org/10.1109/TSG.2016.2523515

Zografopoulos, I., Hatziargyriou, N. D., & Konstantinou, C. (2023). Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations. *IEEE Systems Journal*, *17*(4), 6695–6709. https://doi.org/10.1109/JSYST.2023.3305757

Appendix

Table A1. Abbreviations.

Abbreviation	Full form
CDN	Content Delivery Network
CIA	Confidentiality, Integrity, and Availability
DER	Distributed Energy Resources
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNSSEC	Domain Name System Security Extension
DoS	Denial of Service
DRP	Disaster Recovery Plan
EVCS	Electric Vehicle Charging Station
FMEA	Failure Modes and Effects Analysis
GDPR	General Data Protection Regulation
ICS	Industrial Control System
IDS	Intrusion Detection System
IDPS	Intrusion Detection and Prevention System
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT-GRC	Information Technology Governance, Risk, and Compliance
KPI	Key Performance Indicator
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
NAT	Network Address Translation
NCCS	Network Code for Cyber Security
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NIST	National Institute of Standards and Technology
OT	Operational Technology
PIMS	Privacy Information Management System
PIN	Personal Identification Number
RFID	Radio Frequency Identification
SOCI Act	Security of Critical Infrastructure Act
UEBA	User and Entity Behavior Analytics