Mikko Suorsa

Strengthening Information Security Resilience in the European Energy Retail Sector

A Multi-Method Study of Cultural Factors, Critical Controls, and Key Risks

ACTA WASAENSIA 582

University of Vaasa
VAASAN YLIOPISTO

ISBN 978-952-395-263-8 (print)
978-952-395-264-5 (online)

ISSN 0355-2667 (Acta Wasaensia 582, print)
2323-9123 (Acta Wasaensia 582, online)

URN https://urn.fi/URN:ISBN:978-952-395-264-5

PunaMusta Oy, Joensuu, 2026.

ACADEMIC DISSERTATION

To be presented, with the permission of the Board of the School of Technology and Innovations of the University of Vaasa, for public examination on the 8th of June, 2026, at noon.

Article based dissertation, School of Technology and Innovations, Industrial Management

Author	Mikko Suorsa https://orcid.org/0000-0002-1649-4223
Supervisors	Professor Petri Helo University of Vaasa. School of Technology and Innovations, Industrial Management.
	Dr Jyri Naarmala, University Lecturer University of Vaasa. School of Technology and Innovations, Industrial Management.
Custos	Professor Petri Helo University of Vaasa. School of Technology and Innovations, Industrial Management.
Reviewers	Associate Professor Jonna Järveläinen University of Jyväskylä, Faculty of Information Technology, Information Systems Science.
	Professor Tatiana Welzer-Druzovec University of Maribor, Faculty of Electrical Engineering and Computer Science.
Opponent	Professor Kimmo Halunen University of Oulu, Faculty of Information Technology and Electrical Engineering. National Defence University of Finland, Department of Military Technology.

Tiivistelmä

Energia-alan myyntisektori on kriittinen osa energiateollisuuden arvoketjua, sillä se tuottaa keskeisiä palveluja kuluttajille, yrityksille ja julkisille organisaatioille. Sektori on altis vakaville kyberuhille, joita voimistavat geopoliittiset jännitteet, valtiollisten toimijoiden tukemat kyberhyökkäykset, monimutkaiset järjestelmäarkkitehtuurit sekä tiukka sääntely, kuten Euroopan unionin GDPR (General Data Protection Regulation) ja NIS2-direktiivi (Network and Information Security Directive 2). Näistä haasteista huolimatta empiirinen tutkimus siitä, miten organisaatiokulttuuri, kriittiset tietoturvakontrollit ja riskienhallinta yhdessä vahvistavat kyberturvallisuuden resilienssiä IT-hallinnon, riskienhallinnan ja vaatimustenmukaisuuden (IT Governance, Risk Management and Compliance, IT-GRC) viitekehyksessä, on puutteellista.

Tämä väitöskirja vastaa tunnistettuun tutkimustarpeeseen monimenetelmällisellä tutkimusasetelmalla, joka koostuu neljästä toisiinsa kytkeytyvästä osatutkimuksesta. Tutkimus sisältää tapaustutkimuksen eurooppalaisen energiayhtiön tietoturvakulttuurista henkilöstökyselyjen ja eksploratiivisen faktorianalyysin avulla sekä sisäisesti raportoitujen tietoturvapoikkeamien analyysin hyödyntäen vika- ja vaikutusanalyysiä sekä bow-tie-mallinnusta. Lisäksi väitöskirja tarkastelee toimialarajat ylittävästi GDPR-seuraamusraportteja juurisyyanalyysin keinoin.

Tulokset osoittavat, että kyberturvallisuuden resilienssi edellyttää johdon vahvaa sitoutumista, selkeitä vastuita sekä henkilöstön kannustamista riski- ja tietoturvapoikkeamien raportointiin. Kriittiset tietoturvapuutteet liittyvät erityisesti pääsynhallintaan, korkean käyttöoikeustason valvontaan, tietojärjestelmien elinkaaren muutostenhallintaan, tietoturvatestaukseen, haittaohjelmasuojaukseen, henkilöstön tietoisuuteen ja koulutukseen, turvalliseen tiedonkäsittelyyn sekä tietoturvapoikkeamien kokonaisvaltaiseen hallintaan.

Tutkimus tunnistaa kahdeksan energia-alan myyntisektorille tyypillistä kyberriskiä ja osoittaa, että kerrokselliset kontrollit sekä hyökkäys–puolustus-mallinnus vahvistavat riskienhallintaa ja organisaation tilannekuvaa. Väitöskirja edistää IT-GRC -teoriaa tarjoamalla integroivan viitekehyksen, joka yhdistää organisaatiokulttuurin, kontrollit ja sektorikohtaiset riskit. Tulokset tarjoavat yritysjohdolle konkreettisia keinoja vahvistaa kyberturvallisuuden resilienssiä strategisen ohjauksen, korkean prioriteetin tietoturvakontrollien ja sektorikohtaisten riskien hallinnan avulla.

Asiasanat: tietoturvan johtaminen, kyberturvallisuuden resilienssi, energia-alan myyntisektori, kriittisen infrastruktuurin suojaus, tietoturvakulttuuri, IT-hallinto, riskienhallinta ja vaatimustenmukaisuus, GDPR, ISO/IEC 27001, vika- ja vaikutusanalyysi, bow tie -mallinnus.

Abstract

The energy retail sector provides essential services to consumers, businesses, and public organizations, and constitutes a critical part of the energy industry's value network. It faces sophisticated cyber threats that may disrupt operations, compromise customer data, and cause financial, reputational, and societal harm. These challenges are intensified by geopolitical instability, state-sponsored cyberattacks, complex system architectures, and stringent regulatory requirements, including the EU General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NIS2).

Despite these pressures, empirical research adopting an IT Governance, Risk Management, and Compliance (IT-GRC) perspective on how organizational culture, critical security controls, and sector-specific risks jointly strengthen information security resilience in energy retail remains limited. This dissertation addresses this gap through four interconnected studies: a case study of a European energy retailer examining security culture using survey data and exploratory factor analysis; an analysis of internally reported incidents employing failure modes and effects analysis and bow-tie modelling; and a cross-sector review of GDPR penalty decisions using root cause analysis.

The findings demonstrate that cybersecurity resilience depends on strong leadership commitment, clearly defined responsibilities for risk and incident reporting, and the integration of employee accountability and recognition into performance management. Critical control weaknesses—most notably in access management, privileged access controls, system lifecycle change management, security testing, malware protection, employee awareness and training, secure information handling, and comprehensive incident reporting and response—constitute primary sources of failure.

The study identifies eight cybersecurity risk categories specific to the energy retail sector and shows that layered controls, combined with attack–defence modelling, enhance risk management and organizational situational awareness. The dissertation advances IT-GRC theory by offering an integrative framework that links organizational culture, security controls, and sector-specific risks. The findings provide senior leadership with a concrete roadmap for strengthening cybersecurity resilience through strategic governance, high-priority security controls, and sector-aligned risk management across technical, human, and organizational domains.

Keywords: information security governance, cybersecurity resilience, energy retail, critical infrastructure protection, information security culture, IT-GRC; GDPR, ISO/IEC 27001, FMEA, bow-tie modelling.

ACKNOWLEDGEMENT

I am very grateful to Professor Petri Helo, my supervisor, for his guidance, insight, and constant support throughout my doctoral studies. I also wish to thank Jonna Järveläinen and Tatiana Welzer-Druzovec for reviewing my dissertation and providing valuable feedback that strengthened this work. I am grateful to the case organization for providing the essential data for this research and to the Merchant Gustaf Svanljung Foundation for its generous financial support.

My sincere appreciation goes to Joni Petman for his expert assistance with the statistical analyses, to Christina Gustafsson for her statistical advice, and to John Shepherd for reviewing the language and grammar of this dissertation. I am especially thankful to Aina Špaca for her steadfast encouragement, and to all those who have cheered me on throughout the journey of "taking care of business in a flash."

In Berlin,

Mikko Suorsa

Contents

Figures

Tables

Abbreviations

APPI	Act on Protection of Personal Information (Japan)
CCPA	California Consumer Privacy Act
CIA	Confidentiality, Integrity, and Availability
COBIT	Control Objectives for Information and Related Technologies
DER	Distributed Energy Resource
DSO	Distribution System Operator
EFA	Exploratory Factor Analysis
EU	European Union
FMEA	Failure Modes and Effects Analysis
GDPR	General Data Protection Regulation
IIoT	Industrial Internet of Things
ISMS	Information Security Management System
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IT	Information Technology
IT-GRC	Information Technology Governance, Risk Management, and Compliance
LGPD	Lei Geral de Proteção de Dados (Brazil)

NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NIS	Network and Information Security Directive
NIS2	Network and Information Security 2 Directive
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
OT	Operational Technology
PDPB	Personal Data Protection Bill (India)
PII	Personally Identifiable Information
RCA	Root Cause Analysis
SOCI	Security of Critical Infrastructure Act (Australia)
TSO	Transmission System Operator

Publications

[1] Suorsa, M., Helo, P., & Petman, J. (2025). *Key drivers of information security culture: A survey and exploratory factor analysis in an energy retail organization* [Manuscript submitted for publication]. *Information Security Journal: A Global Perspective*. © 2025 The Author(s). This manuscript is included in the dissertation with the permission of the co-authors.

[2] Suorsa, M., & Helo, P. (2023). *Information security failures identified and measured: ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis* [Peer-reviewed journal article]. *Information Security Journal: A Global Perspective, 33*(3), 285–306. https://doi.org/10.1080/19393555.2023.2270984. © 2023 Taylor & Francis Group, LLC. Reproduced with permission in accordance with the publisher's dissertation reuse policy.

[3] Suorsa, M., & Helo, P. (2023). *Information security failures measured and ISO/IEC 27001:2022 controls ranked by General Data Protection Regulation penalty analysis* [Conference paper]. In *Proceedings of the 2023 11th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1–5). Makassar, Indonesia. https://doi.org/10.1109/CITSM60085.2023.10455413. © 2023 IEEE. Reprinted with permission in accordance with IEEE thesis reuse guidelines.

[4] Suorsa, M., & Helo, P. (2025). *Cybersecurity risks and defense for a European energy retail business: A case study using FMEA and Bowtie incident analysis* [Peer-reviewed journal article]. *Information Security Journal: A Global Perspective*, 1–29. https://doi.org/10.1080/19393555.2025.2489421. © 2025 Taylor & Francis Group, LLC. Reproduced with permission in accordance with the publisher's dissertation reuse policy.

1 INTRODUCTION

Energy retail operations, which supply energy products and services to consumers, businesses, and public organizations, deliver essential services to society and constitute a critical sector of the energy industry value network (European Parliament & Council of the European Union, 2022). Their significance is underscored by the fact that nearly all critical societal functions depend on a resilient and reliable energy supply (Löschel et al., 2010), reflecting modern life's fundamental reliance on continuous energy availability (Saeed et al., 2024).

Interruptions in the energy sector can disrupt core societal functions, including healthcare, public safety and emergency services, water and sanitation, food distribution, transportation, communications and IT infrastructure, financial services, government operations, and national security (Gouglidis, 2018). These cascading impacts highlight the potentially severe consequences of energy supply failures across interconnected systems and critical infrastructure (Jasiūnas et al., 2021).

Cybersecurity threats in the energy sector are particularly severe. Successful attacks can result in operational shutdowns, financial losses, data breaches, legal liabilities, and reputational damage (Falowo et al., 2022). As one of an organization's most valuable and strategically important assets, information becomes vulnerable when appropriate security controls are inadequate, potentially affecting both operational stability and organizational continuity (Gerber & von Solms, 2008).

Materialized cybersecurity threats can also cause financial harm and psychological distress to customers, particularly when personally identifiable information (PII) is compromised by malicious actors (Agrafiotis et al., 2018). These impacts emphasize the necessity of information security in safeguarding critical infrastructure (Yusta et al., 2011) and underline its role as a fundamental resilience factor within the energy retail sector (Azzuni & Breyer, 2017), which has become a high-value target for cybercriminals due to its substantial financial significance (Dagoumas, 2019).

Notable incidents against energy infrastructure illustrate the severity of these threats. In 2020, a cyberattack on Energias de Portugal resulted in the loss of ten terabytes of sensitive data, along with significant financial and reputational damage (Truță, 2020). The 2015 cyberattacks on Ukraine's power grid caused widespread outages, demonstrating the use of cyberattacks as an instrument of hybrid warfare (Whitehead et al., 2017), while the 2013 Bowman Avenue Dam intrusion in New York revealed further vulnerabilities in critical infrastructure (Hassanzadeh et al., 2020).

Over the decades, cyberattacks have evolved from isolated criminal acts to state-sponsored cyberterrorism (Ang & Utomo, 2017). This evolution has been driven by rapid technological advances, including artificial intelligence–guided attacks and cyberattacks-as-a-service, which increase threat frequency and sophistication, challenge security defenses, elevate breach risks in complex systems, and complicate detection (Guembe et al., 2022; Mallick & Nath, 2024). Reflecting these trends, the World Economic Forum's Global Cybersecurity Outlook 2025 reports that 72% of organizations experience heightened cyber risks (Jurgens & Dal Cin, 2025).

In consequence, strengthening the resilience of energy companies has become a global priority (Venkatachary et al., 2017), with urgency rising amid escalating geopolitical tensions and the growing sophistication of cyberattacks targeting energy infrastructure worldwide (Aljohani, 2024). Efforts to ensure the protection of the sector have also driven a legislation-driven megatrend (Haber & Zarsky, 2018), resulting in increasingly complex information security compliance requirements (Gerber & von Solms, 2008).

This is evident in the European Union (EU), where the General Data Protection Regulation (GDPR), effective from 2018, requires organizations to safeguard citizens' privacy through adequate information security measures. Member states' supervisory authorities oversee compliance and may impose fines of up to €20 million or 4% of global turnover (European Parliament & Council of the European Union, 2016). For example, in 2021, the Italian Data Protection Authority fined Enel Energia SpA €79.1 million for weak access controls and credential management, resulting in the loss of PII confidentiality (CMS Law, 2022).

Another major regulation exemplifying this megatrend is the Directive on Security of Network and Information Systems 2 (NIS2), which entered into force in the EU in January 2023. Under NIS2, energy retailers are classified as essential entities and must comply with information security requirements, including risk analysis, incident reporting, business continuity, disaster recovery, and supplier management, all overseen by organizational executives. Unlike the GDPR, NIS2 also holds the executive leadership personally accountable for compliance (European Parliament & Council of the European Union, 2022).

A comprehensive approach is central to strengthening information security resilience (Soomro et al., 2016), defined as an organization's ability to prepare for, withstand and recover from cyber incidents, adapt to evolving threats, and sustain essential business operations (Ross et al., 2021; Björck et al., 2015). This integrated, enterprise-wide perspective aligns with von Solms's (2006) conceptualization of the Fourth Wave of information security. It moves beyond technical controls to include organizational culture, corporate governance, legal compliance, top management

commitment, organizational structures, policies, user awareness, and the management of both technical and human risks. Within this context, IT governance, risk management, and compliance (IT-GRC) functions are instrumental in enabling and sustaining resilient information security practices (Halliday, 2024; Meagher & Dhirani, 2024).

Information security resilience within IT-GRC depends on cultivating a well-developed organizational culture, which guides strategic priorities and promotes secure practices, thereby strengthening the organization's overall security posture (Adeyinka et al., 2024; da Veiga & Eloff, 2010). Given that technological safeguards alone are insufficient, organizations need to foster a culture in which employees internalize, adopt, and consistently apply secure practices, reinforcing organizational resilience (Tang et al., 2016; Mahfuth et al., 2017).

The development of information security culture has been widely studied (Alnatheer, 2015; Sherif et al., 2015; Uchendu et al., 2021), while top management engagement is consistently identified as a key factor (Vincent et al., 2019; Cuganesan et al., 2018). However, the effects of factors beyond management commitment, and the mechanisms through which they influence culture, are not yet fully understood. Further research is needed to clarify these dynamics and inform more resilient organizational strategies (Gcaza & von Solms, 2017; AlHogail & Mirza, 2014), emphasizing cultural factors as critical success elements in IT-GRC (Gericke et al., 2009).

Further key success factors for IT-GRC include gathering intelligence on information security failures and compliance breaches, and implementing corresponding controls to manage them effectively (von Solms, 2006). This is particularly important for bridging the gap between complex regulatory requirements and day-to-day information security practices (Dlamini et al., 2009), especially as authorities adopt stricter enforcement, leading to increasingly severe penalties for non-compliance (Barrett, 2020).

In this context, international standardization frameworks are essential for governing, guiding, and certifying resilient information security practices (Siponen & Willison, 2009). ISO/IEC 27001, in particular, is widely recognized as the de facto standard for systematically managing information security and implementing critical controls (Calder & Gerard, 2013). Nevertheless, identifying, prioritizing, and selecting the most important and interconnected controls remains challenging in highly networked organizational environments (Tariq et al., 2020), highlighting the need for intelligence to inform IT-GRC decision-making (Vaibhav, 2022).

Furthermore, strengthening information security resilience within IT-GRC relies on systematically learning from cybersecurity incidents to identify, assess, and mitigate associated risks (Patterson et al., 2023; Ebert et al., 2023). This is particularly challenging in energy retail due to its complex systems and process landscape (Ridha et al., 2020) and may be further complicated by the scarcity of concrete incident data (Maschmeyer et al., 2020; Eling & Wirfs, 2019). These constraints underscore the need for further research into the causes, effects, and risk mitigation strategies of cybersecurity incidents (Al-Mhiqani et al., 2018) in energy retail.

Building on these challenges, cybersecurity incidents are often highly complex, requiring advanced techniques to identify and analyze attack patterns and defense mechanisms (Staheli et al., 2014; de Ruijter & Guldenmund, 2016). While evolving information security regulations increasingly require executive oversight, graphical attack-defense visualization models have proven effective for analyzing and communicating these risks (Moody, 2007; Carlson, 2012).

Despite the general focus on IT-GRC in the retail sector (Vaka, 2025; Ardhaninggar & Ramli, 2024; Symantec, 2024; Amosu et al., 2024), integrative empirical research specifically examining energy retail operations remains limited. Most studies address it only briefly within broader analyses of the energy value network (Gong & Lee, 2021; Nikolaou et al., 2023) or in customer-focused research on distributed energy resources (DERs) (Zografopoulos et al., 2023).

Furthermore, while information security has been studied in energy generation (Bıçakcı & Evren, 2022; Lee et al., 2023), grid operations (Wang & Lu, 2013; Sun et al., 2018), and other critical industries (Ani et al., 2016; Salama et al., 2024; Shoetan et al., 2024; Almudaires & Almaiah, 2021; Kulkarni et al., 2024; Ukwandu, et al., 2022), focused studies on energy retail remain scarce. This highlights the need for dedicated research to understand how comprehensive IT-GRC approaches can strengthen information security resilience in this critical sector.

1.1 Research problem

The energy retail sector is essential to the core functions of society and critical infrastructure, yet it faces increasingly sophisticated cyber threats that can disrupt operations, compromise customer data, and cause significant financial and reputational harm. These risks are amplified by escalating geopolitical tensions, hybrid warfare, and state-sponsored cyberattacks, and are further challenged by complex system architectures, rapidly evolving attack techniques, and stringent regulatory requirements such as the GDPR and NIS2, which demand greater resilience, compliance, and executive accountability.

Despite the sector's high importance, empirical understanding remains limited with regard to how organizational culture, the implementation and effectiveness of critical information security controls, and sector-specific cybersecurity risks interact to shape resilience in energy retail. While IT governance, risk, and compliance (IT-GRC) frameworks such as ISO/IEC 27001 provide formal guidance for managing information security risks, nevertheless control failures, recurring incidents, and data breaches continue to occur, highlighting persistent gaps between policy and practice.

Moreover, the limited availability of sector-specific incident data and the scarcity of empirical studies on energy retail constrain the development of integrated, risk-based, and resilient cybersecurity practices. This constitutes a significant research problem, as it limits comprehensive understanding of three key domains essential to strengthening information security resilience: (1) cultural factors that drive secure behavior, (2) critical controls and their effectiveness in addressing security shortcomings, and (3) key sector-specific cybersecurity risks and the corresponding strategies for their management. Addressing these gaps is fundamental to developing actionable, empirically grounded practices that strengthen information security resilience in the European energy retail sector.

1.2 Research aim, questions and design

This dissertation investigates information security culture, critical controls, and sector-specific cybersecurity risks in the European energy retail sector, with the aim of strengthening integrated, risk-based, and resilient cybersecurity practices. Guided by an interpretivist, inductive, and exploratory research philosophy, the study employs qualitative and quantitative methods across four interrelated research papers, hereafter referred to as Paper I, Paper II, Paper III, and Paper IV, to examine how organizational culture, the effectiveness of critical controls, and sector-specific risks interact to shape information security resilience.

The study integrates survey research, archival analysis, and internal incident data analysis, employing analytical techniques such as Exploratory Factor Analysis (EFA), Root Cause Analysis (RCA), Failure Modes and Effects Analysis (FMEA), and bow-tie modeling. This multi-method approach enables the triangulation of insights from employee perceptions, regulatory enforcement cases, and internal incident reports, providing an evidence-based foundation for theory-building and actionable recommendations.

Paper I focuses on information security culture, exploring the factors and mechanisms that drive its development and reinforcement within energy retail organizations. The research question guiding this study is:

- RQ1: What are the key factors that drive the strengthening of information security culture in energy retail organizations?

Paper I employed a survey-based, single-case design targeting employees within a large European energy retail organization. Data were collected using a structured questionnaire, which was sent to 2,100 employees, yielding 610 responses for a 29% response rate. The responses were analyzed using exploratory factor analysis (EFA) to identify the latent dimensions of information security culture.

Papers II and III investigate critical controls, examining recurring failures and their impact on information security resilience. Paper II analyzes archival data from 81 GDPR Article 32 penalty cases (2020), mapped to ISO/IEC 27001:2013 controls, while Paper III updates the analysis to reflect the ISO/IEC 27001:2022 standard. The research questions addressed in these papers are:

- RQ2: What are the most frequent and most expensive information security failures corresponding to ISO 27001 controls?
    - RQ2.1: How many information security failures corresponding to ISO 27001 controls typically exist in a GDPR penalty case?
    - RQ2.2: How do the information security failures corresponding to ISO 27001 controls correlate?
    - RQ2.3: Are there any industry type differences in information security failures and penalties?
    - RQ2.4: What are the most frequent and most expensive information security failures corresponding to ISO/IEC 27001:2022 controls, and what is their correlation?

The analyses in Papers II and III combined RCA with statistical techniques to identify failure patterns, control gaps, and sector-specific variations, providing insights into the effectiveness of critical controls. Building on the same case organization as Paper I, Paper IV investigates key cybersecurity risk categories, failure modes, their effects, and mitigation strategies within the operational and regulatory context, extending the analysis to risk management practices. The research questions for this study are:

- RQ3: What are the main cybersecurity risk categories for the energy retail business?
    - RQ3.1: What are the cybersecurity failure modes, effects, and corresponding mitigation measures for the energy retail business?

- RQ3.2: How can graphical attack modeling techniques enhance cybersecurity risk management for the energy retail business?

Paper IV employs a single-case, longitudinal design, analyzing six years of internal cybersecurity incident reports (2018–2023). FMEA was used to systematically categorize and assess risks, while bow-tie modeling exemplified graphical visualization of the relationships between threats, controls, and potential consequences.

Table 1. Papers I–IV: research objectives, questions and study design

Paper	Objective	Main RQ	Sub-RQ	Study design
I	Examine factors and mechanisms that strengthen information security culture in energy retail organizations.	RQ1: What are the key factors that drive the strengthening of information security culture in energy retail organizations?	-	Survey-based, single-case study of a large European energy retailer, sent to 2.100 employees, yielding 610 responses (29% response rate) and analyzed using EFA.
II	Analyze recurring ISO/IEC 27001:2013 control failures in GDPR penalty cases and their impact on resilience.	RQ2: What are the most frequent and most expensive information security failures corresponding to ISO 27001 controls?	RQ2.1: How many information security failures corresponding to ISO 27001 controls typically exist in a GDPR penalty case? RQ2.2: How do the information security failures corresponding to ISO 27001 controls correlate? RQ2.3: Are there any industry type differences in information security failures and penalties?	Archival analysis of 81 GDPR Article 32 penalty cases (2020), mapped to ISO/IEC 27001:2013 controls. RCA and statistical techniques applied.
III	Extend analysis to ISO/IEC 27001:2022 controls and their correlations.	-	RQ2.4: What are the most frequent and most expensive information security failures corresponding to ISO/IEC 27001:2022 controls, and what is their correlation?	Re-analysis of the GDPR dataset from Paper II according to ISO/IEC 27001:2022 controls. RCA and statistical techniques applied.
IV	Investigate key cybersecurity risk categories, failure modes, and mitigation strategies in energy retail.	RQ3: What are the main cybersecurity risk categories for the energy retail business?	RQ3.1: What are the cybersecurity failure modes, effects, and corresponding mitigation measures for the energy retail business? RQ3.2: How can graphical attack modeling techniques enhance cybersecurity risk management for the energy retail business?	Single-case, longitudinal study (2018–2023) of a large European energy retailer using internal incident reports, FMEA, and bow-tie modeling.

Table 1 provides an overview of Papers I–IV, summarizing their research objectives, questions, and study design. It demonstrates how the dissertation synthesizes multiple perspectives on organizational culture, regulatory compliance, critical controls, and sector-specific cybersecurity risks to advance both the understanding of and the strengthening of information security resilience in the European energy retail sector.

2 LITERATURE AND CONCEPTUAL FOUNDATION

This chapter provides an overview of the literature and the conceptual foundation of the dissertation, based on a synthesis of peer-reviewed studies, industry standards, and regulatory developments. The study is positioned within industrial management research, reflecting the transformation of the energy sector under Industry 4.0, where the convergence of physical, digital, and human technologies introduces complex operational risks (Lezzi et al., 2018). In this context, these risks can be managed through quality management principles and standardization frameworks that integrate regulatory compliance with measurable performance and continuous improvement practices (Fiore et al., 2023).

Table 2. Overview of key research domains

Research domain	Key concepts	Seminal references	Relevance
IT governance, risk management, and compliance (IT-GRC)	Governance, risk management, compliance (strategy, policies, leadership; risk assessment, mitigation; regulatory adherence)	von Solms, 2000; Vicente & da Silva, 2011; Soomro et al., 2016	Provides a structured, proactive approach to strategy, risk mitigation, oversight, and compliance.
Information security and cybersecurity resilience	CIA triad, security evolution, cybersecurity threats (ransomware, phishing, IT–OT vulnerabilities)	Stewart et al., 2012; von Solms, 2000, 2006, 2010; Lundgren & Möller, 2019	Highlights the evolution of information security and need for integrated technical, organizational, and cultural resilience.
Regulatory landscape	GDPR, NIS2, EU Cyber Resilience Act	European Parliament & Council of the European Union, 2016, 2022; Ruohonen & Hjerppe, 2022	Shows how complex regulation shapes organizational IT-GRC practices and compliance requirements.
Information security standardization frameworks	ISO/IEC 27001, ISO/IEC 27002, NIST CSF	ISO, 2013, 2022a, 2022b; Sulistyowati et al., 2020	Provides structured guidance for implementing IT-GRC and risk-based ISMS.
Information security culture	Management engagement, awareness, policy compliance, trust, teamwork, reporting	Papazafeiropoulou & Spanaki, 2015; Gcaza & von Solms, 2017; Georgiadou et al., 2022	Emphasizes the role of culture as a driver of IT-GRC and organizational resilience.
Energy retail and energy industry value network	Generation, grid, retail, DERs, IT–OT convergence, customer data	Demirel, 2012; Bıçakcı & Evren, 2022; Nazari & Musilek, 2023	Identifies sector-specific operational and cybersecurity risks, highlighting the importance of resilience in energy retail.
Cross-sector critical infrastructure studies	Resilience practices (continuity planning, alertness, dynamic capabilities)	Ani et al., 2016; Järveläinen, 2013; Niemimaa et al., 2019	Offers insights from other sectors to guide resilience practices in energy retail.

The conceptual foundation highlights the interconnections among governance, risk management, compliance, technical standards, organizational culture, and sector-specific characteristics. It also identifies gaps in empirical research, particularly

regarding the practical implementation of IT-GRC and resilience mechanisms in energy retail. To provide a comprehensive overview of the multidimensional factors shaping information security resilience, Table 2 summarizes the main research domains, key concepts, seminal references, and their relevance to the European energy retail sector.

This chapter is organized as follows. It first reviews the evolution of information security and cybersecurity resilience (Section 2.1), followed by the regulatory landscape (Section 2.2), standardization frameworks (Section 2.3), organizational culture (Section 2.4), and the energy retail sector within the energy industry value network (Section 2.5). Comparative studies from other critical infrastructures are then examined (Section 2.6), concluding with a conceptual synthesis (Section 2.7) that highlights the empirical gaps addressed by this dissertation.

2.1 Information security and cybersecurity resilience

In this dissertation, the terms cybersecurity and information security are used interchangeably. Both appear in professional literature and cover the full spectrum of relevant domains (Stewart et al., 2012). While cybersecurity is often considered a broad concept that primarily focuses on the digital realm, information security encompasses both the digital and physical dimensions of information (von Solms & von Solms, 2018).

Information security is traditionally defined through the CIA triad, where confidentiality restricts access to authorized users, integrity ensures the accuracy and completeness of information, and availability guarantees timely access (Stewart et al., 2012). While foundational, this model, originating in U.S. military and government practices of the 1970s, offers only a partial view, as it overlooks human and organizational factors and therefore lacks the flexibility and contextual depth required in contemporary settings (Lundgren & Möller, 2019).

Building on these foundational concepts, information security has evolved through successive “waves” that progressively broaden its scope and practical application across organizations. The Technical Wave focused on technical controls, the Management Wave integrated security into organizational processes, and the Institutional Wave emphasized standards, corporate culture, and continuous measurement, reflecting a more professionalized and holistic approach (von Solms, 2000).

The current Fourth Wave extends this evolution by incorporating corporate governance, legal compliance, top management commitment, organizational culture,

and formal policies, thereby addressing both technical and human risks across the organization (von Solms, 2006). Building on this governance-oriented foundation, the Fifth Wave of cybersecurity shifts the focus to internet-enabled threats, requiring organizations to move beyond internal controls toward proactive prevention of cybercrime and user protection in increasingly interconnected digital environments (von Solms, 2010).

Within this landscape of escalating cyber threats and expanding regulatory requirements, IT governance, risk management, and compliance (IT-GRC) has become central to the development of resilient information security practices. Rather than a purely technical function, IT-GRC represents a multidimensional discipline that integrates governance structures, risk-based decision-making, and compliance mechanisms to support organizational resilience (Soomro et al., 2016; von Solms, 2001; Nicho et al., 2017).

In IT-GRC, Governance guides strategy, objectives, organizational culture, risk appetite, and formal policies, providing a structured framework for decision-making and organizational direction (Vicente & da Silva, 2011). Risk Management systematically identifies, assesses, and mitigates potential threats to organizational assets and operations (Wright, 2019), while Compliance ensures adherence to laws, regulations, and standards, reducing legal, financial, and reputational risks and fostering confidence and trust among internal and external stakeholders (Adeyinka et al., 2024).

Together, these interrelated functions establish an integrated approach to securing information and maintaining organizational resilience, which is defined as an organization's ability to prepare for, withstand, recover from, and adapt to cyber incidents while sustaining essential business operations (Ross et al., 2021; Björck et al., 2015). Unlike traditional business continuity, which primarily focuses on post-incident recovery, information security resilience emphasizes continuous preparedness, adaptive capacity, and proactive prevention or mitigation of potential incidents before they materialize (Herbane et al., 2004; Järveläinen, 2013).

2.2 Evolution of information security regulation

Since the early 21st century, the European Union has prioritized the protection of critical infrastructures through comprehensive information security legislation (Bederna & Rajnai, 2022). Recent initiatives, such as the European Cyber Resilience Act (Regulation (EU) 2024/2847, 2024), the Network Code on Cybersecurity for the Electricity Sector (Commission Delegated Regulation (EU) 2024/1366, 2024), and the EU Artificial Intelligence Act (Regulation (EU) 2024/1689, 2024), collectively

reflect the EU's comprehensive approach to securing digital and industrial ecosystems.

Among these legislative efforts, the General Data Protection Regulation (GDPR), in force since May 2018, has been particularly influential for the energy retail sector. It safeguards EU citizens' right to data protection by regulating how organizations process personal data and granting individuals greater control over its use. Central to the GDPR is information security: Article 32, "Security of Processing," requires organizations to implement appropriate technical and organizational measures to protect personal data. Failure to comply can result in significant penalties, as supervisory authorities may impose fines of up to €20 million or 4% of global turnover (European Parliament & Council of the European Union, 2016).

Although relatively recent, GDPR enforcement has already been the focus of scholarly investigation. Ruohonen & Hjerppe (2022) find that enforcement most often cites articles on general principles, lawfulness, and information security. Presthus & Sønslien (2021) identify common violations, note rising fines, and highlight the regulation's practical complexity. Akhlaghpour et al. (2021) identify risk categories and mitigation measures in GDPR cases, while Wolff & Atallah (2021) note that early fines were modest, with more substantial penalties primarily imposed for breaches of information security.

Similar regulatory initiatives have emerged worldwide, reflecting a growing megatrend toward enhanced information security and personal data protection. Notable examples include the California Consumer Privacy Act (CCPA) (Thomas, 2020), Brazil's Lei Geral de Proteção de Dados (LGPD) (Macedo, 2021), India's Personal Data Protection Bill (PDPB) (Deva & Suchithra, 2020), and Japan's Act on Protection of Personal Information (APPI) (Higashizawa & Aihara, 2017).

Alongside data protection laws, sector-specific cybersecurity directives have further enhanced resilience, with the Network and Information Security 2 Directive (NIS2 Directive) serving as a key example. Building on the original Network and Information Security Directive (NIS Directive), the NIS2 Directive extends cybersecurity measures across essential sectors. In the energy industry, while the original NIS Directive covered only electricity, gas, and oil production, transmission, and storage, NIS2 expands its scope to include energy retail companies, recognizing their critical role in the energy value network and ensuring the continuity of essential services for society (European Parliament & Council of the European Union, 2022; Directive (EU) 2016/1148, 2016).

NIS2 mandates a risk-based information security management approach, requiring risk analysis, incident management, business continuity, disaster recovery, and

supplier assessments, all overseen by the leadership of energy companies. Significant incidents affecting essential services must be reported, and service recipients notified. Company leaders can be held liable for violations, and enforcement includes fines of up to €10 million or 2% of worldwide turnover, underscoring the critical importance of cybersecurity risk management and incident oversight (European Parliament & Council of the European Union, 2022).

Similar developments to NIS2 reflect a broader global megatrend of strengthening cybersecurity and resilience for critical infrastructure. Examples include the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards (Dolezilek & Hussey, 2011), the Australian Security of Critical Infrastructure Act (SOCI Act) (Shah, 2023), and the Critical Infrastructure Protection Act in South Africa (Calandro, 2020).

2.3 Information security standardization frameworks

International standardization frameworks provide the foundation for governing, assuring, and certifying effective information security in organizations (Siponen & Willison, 2009). They apply quality management principles to ensure consistent processes, continuous improvement, risk mitigation, and compliance, thereby enhancing organizational performance (Fiore et al., 2023). Additionally, these standards offer structured guidance and certification-based mechanisms for systematic risk identification, assessment, and mitigation, supporting a core component of IT-GRC (Björnsdóttir et al., 2022; Wright, 2019).

Information security standards differ in specificity, serving both general and industry-specific purposes, while supporting diverse compliance requirements (Syafrizal et al., 2020). Among these, ISO/IEC 27001, alongside frameworks such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and Control Objectives for Information and Related Technologies (COBIT), is one of the most widely adopted (Sulistyowati et al., 2020; Dharmalingam et al., 2018) and recommended (Mayer & De Smet, 2017; Brenner, 2007) due to its comprehensive approach, which enables structured IT-GRC implementation (Choubey & Bhargava, 2018).

Specifically, ISO/IEC 27001:2013 defines requirements for establishing, implementing, and maintaining a risk-based information security management system (ISMS) and provides controls for managing risks (International Organization for Standardization [ISO], 2013). The ISO/IEC 27001:2022 update modernizes these controls (International Organization for Standardization [ISO], 2022a), while ISO/IEC

27002:2022 provides detailed guidance for their effective implementation (International Organization for Standardization [ISO], 2022b).

Together, these standards are complementary, with ISO/IEC 27001 establishing the ISMS framework, and ISO/IEC 27002 guiding the practical application and operationalization of controls. Additionally, ISO/IEC 27002:2019 offers supplementary guidelines for implementing privacy and security controls (International Organization for Standardization [ISO], 2019). Overall, these standards function as compliance enablers, supporting organizations in meeting privacy and security requirements (Lopes et al., 2019).

In the literature, ISO/IEC 27001 has served as a benchmark for assessing organizational information security maturity. However, most studies offer only limited guidance on improving assessed maturity levels (Anass et al., 2020). While some research has identified key ISO 27001 controls (Shojaie et al., 2014; Khajouei et al., 2017), determining and prioritizing the most critical controls remains a persistent management challenge, especially in complex organizational environments (Tariq et al., 2020). This highlights the ongoing need for informed guidance to bridge the gap between regulatory requirements and the practical prioritization of ISMS controls (Vaibhav, 2022; Dlamini et al., 2009).

2.4 Cultural factors influencing information security

An organization's IT-GRC both shapes and is shaped by its cultural, social, and political environment (Papazafeiropoulou & Spanaki, 2015) and, when effectively implemented, offers numerous organizational benefits (Ali et al., 2021). Understanding compliance principles encourages employees to ask questions, make ethical decisions, and report violations, fostering a positive culture that reinforces shared values and organizational commitment (Schwartz, 2001).

Although prior research has shown that information security culture can vary across subgroups or professional roles (da Veiga & Martins, 2017; Ramachandran et al., 2013), this study focuses on the dominant or shared aspects of security culture within the energy retail organization. This approach assumes a common underlying culture for analytical purposes while recognizing that subcultural differences may exist and could be explored in future research.

Despite many benefits, a common challenge in IT-GRC implementation is the tendency to overlook organizational culture (Adeyinka et al., 2024), which is often complex, difficult to conceptualize, and challenging to measure (Schlaile et al., 2021). If left unmanaged, culture can unconsciously influence organizational processes and

employee behavior, highlighting its importance as a critical success factor in IT-GRC (Gericke et al., 2009).

Many useful frameworks for assessing and improving information security culture have been proposed in the literature (see, for example, da Veiga & Eloff, 2010; Sutton & Tompson, 2025). Among these frameworks, for this dissertation, the Cybersecurity Culture Framework for assessing organizational readiness developed by Georgiadou et al. (2022) is adopted as an analytical lens, through which its identified cultural factors are systematically operationalized in the survey questions.

The current research identifies several key factors that influence the development and reinforcement of information security culture within organizations (Alnatheer, 2015; Sherif et al., 2015; Uchendu et al., 2021). In particular, active and sustained management engagement is consistently highlighted as a critical driver, being instrumental in shaping the organization's overall security culture and guiding employee behavior (Vincent et al., 2019; Cuganesan et al., 2018).

Beyond management engagement, other key contributing factors include employees' security risk perception (Nasir et al., 2019), awareness (Tolah et al., 2021), and policy compliance along with actual behavior (Ali et al., 2021). Additional important factors addressed by the literature include a sense of responsibility (AlHogail, 2015), risk and incident reporting (Ahola et al., 2025), trust (da Veiga et al., 2020), teamwork (Ioannou et al., 2019), and the assessment and recognition of positive behavior (Gravina et al., 2021; Vuong & Nguyen, 2022).

Despite prior research, the precise mechanisms through which these factors shape resilient cybersecurity strategies and organizational behavior remain not fully understood (Gcaza & von Solms, 2017; AlHogail & Mirza, 2014). This highlights the need for further comprehensive and in-depth research on the key drivers of information security culture and their critical role in strengthening organizational resilience, particularly within energy retail organizations.

2.5 Energy industry and retail information security

The energy industry value network begins with energy generation, which utilizes nonrenewable resources such as coal, petroleum, natural gas, and nuclear energy, as well as renewable resources including solar, wind, bioenergy, geothermal, and waste (Demirel, 2012). Cybersecurity in energy generation has been extensively studied because incidents can disrupt operations, endanger human life, compromise safety, and cause serious environmental harm (Bıçakcı & Evren, 2022; Lee et al., 2023; Zhang et al., 2016).

From this generation segment, energy flows through interconnected transmission and distribution segments. Transmission system operators (TSOs) transport large volumes of energy over high-voltage networks to maintain system balance, while distribution system operators (DSOs) deliver energy through medium- and low-voltage networks to end users (Hadush & Meeus, 2018). Given the criticality and interdependence of these segments, cybersecurity within grid operations has been extensively examined (Wang & Lu, 2013; Sun et al., 2018).

In parallel with these physical segments, market mechanisms coordinate economic interactions across the energy industry value network. Energy markets facilitate the trading of electricity, gas, and other energy commodities, enabling price discovery, balancing supply and demand, and promoting efficient resource allocation (Burger et al., 2014). Beyond these operational functions, cybersecurity in energy markets has attracted growing scholarly attention (Afzal et al., 2024; Müller et al., 2023).

Within this interconnected value network, energy retail represents a key, yet comparatively underexplored actor. Retailers manage the sale of electricity, gas, heat, and other energy products and services to households, businesses, and public organizations, while handling large volumes of sensitive customer data. This role exposes them to substantial cybersecurity risks, regulatory challenges, and operational complexities, making energy retail a crucial focus for resilient information security research (Brown et al., 2019; Golmohamadi & Keypour, 2017).

Energy retail organizations face substantial information security challenges, primarily due to their highly digitalized and interconnected operating environments and the large volumes of customer data they process (Nazari & Musilek, 2023). Energy retailers routinely collect and process personally identifiable information (PII), including identity and contact details, financial and billing information, technical and metering data, as well as customer service interactions and behavioral preferences (Klich, 2023).

Furthermore, energy contracts, particularly utility bills, are commonly used as proof of identity or residence in administrative, legal, and financial contexts (UK Government, 2025). This practice increases their attractiveness for misuse and elevates the risk of identity fraud. Despite these elevated risks, research that focuses specifically on information security within the energy retail segment remains limited, with most existing studies addressing retail only as part of broader analyses of the energy industry value network (Gong & Lee, 2021; Nikolaou et al., 2023).

Figure 1 illustrates the classical structure of the energy industry value network, showing the flow from generation through transmission, distribution, and retail to end consumers, alongside market interactions. The figure offers a general overview

of the main segments and interconnections of the energy system, providing context for contemporary topics such as smart grids, DER integration, and cybersecurity. The icons used in the figure are sourced from Flaticon and are licensed under Creative Commons Attribution 3.0.

Figure 1. The energy industry value network

Simultaneously, the energy industry value network is undergoing a fundamental transformation driven by digitalization, decentralization, and increased customer participation. The emergence of smart grids marks a shift from a traditionally centralized energy system with passive consumers to decentralized and flexible architectures that integrate renewable energy sources and empower prosumers, actors who both produce and consume energy (Alam & Shukla, 2022).

Distributed Energy Resources (DERs), including photovoltaic panels, small wind turbines, batteries, inverters, smart meters, and electric vehicle chargers, are becoming increasingly prevalent. Typically located close to the point of consumption and connected either to the distribution grid or behind the customer's meter, DERs enable prosumers to feed electricity into the grid and reduce net consumption, while simultaneously introducing new cybersecurity and data protection risks (Muqeet et al., 2019; Zografopoulos et al., 2023).

Consequently, DER cybersecurity has emerged as a prominent research topic, particularly within the context of Industry 4.0 (Faheem et al., 2018; Sun et al., 2020; Hseiki et al., 2024; Hamdare et al., 2023). This focus reflects the decentralized, interconnected, and interoperable nature of DERs, as well as their customer-facing and remotely controllable characteristics (Zografopoulos et al., 2023). Among DER-related data, smart meter consumption information is especially sensitive, as it can reveal detailed household behaviors, including daily routines, occupancy patterns, and lifestyle characteristics, thereby posing significant challenges for data protection and regulatory compliance (Beckel et al., 2014).

In addition to decentralization, the digital transformation of the energy industry value network is driving the convergence of information technology (IT) and operational technology (OT). Systems that were historically separate are increasingly

interconnected, which expands the cyberattack surface. Vulnerabilities in industrial Internet of Things (IIoT) devices and legacy systems, together with ineffective patch management practices, limited system visibility, and weak collaboration between IT and OT domains, increase the likelihood that malicious actors can successfully compromise energy operations (Jiang et al., 2023; Murray et al., 2017).

Cyberattacks often originate in IT environments and propagate into critical OT systems. A widely cited example is the 2015 Ukraine power grid attack, in which spear-phishing campaigns allowed attackers to access industrial control systems and trigger widespread power outages (Whitehead et al., 2017). This incident highlights the urgent need to strengthen cybersecurity resilience in energy retail, where digitalization, integration across the value network, and sensitive customer data amplify the impact of cyber incidents. Advancing comprehensive risk management and resilient defense strategies in this context is a critical yet underexplored research priority.

2.6 Comparative studies in other critical infrastructures

Information security resilience has been extensively studied across critical sectors, including manufacturing (Ani et al., 2016), healthcare (Salama et al., 2024), telecommunications (Shoetan et al., 2024), payment cards (Almudaires & Almaiah, 2021), food and agriculture (Kulkarni et al., 2024), water systems (Tuptuk et al., 2021), aviation and air traffic management (Ukwandu et al., 2022), and the maritime sector (Abdelmagid et al., 2025). These studies highlight the importance of resilience in protecting organizations and society from operational disruptions, financial losses, regulatory penalties, and reputational damage.

Research indicates that organizational resilience is operationalized in multiple ways, including categorizing ransomware and malware risks by likelihood, impact, and available controls, while larger organizations emphasize continuity practices, situational awareness, and managerial support to mitigate cyber incidents (Javadnejad et al., 2024; Järveläinen, 2013). Cross-sector studies further highlight dynamic capabilities that enable organizations to adapt resources, processes, and strategies to evolving threats and environments, thereby strengthening resilience, decision-making, and long-term performance (Niemimaa et al., 2019; Järveläinen et al., 2025).

For example, hospitals protect patient records and medical devices through continuous monitoring, automated threat detection, and staff training, reflecting risk categorization and continuity measures (Salama et al., 2024). Water utilities employ simulation-based risk assessments and redundancy planning to maintain operational

continuity (Tuptuk et al., 2021), while payment card organizations implement layered security, including encryption, multi-factor authentication, and artificial intelligence driven fraud detection, to safeguard financial data and ensure regulatory compliance (Almudaires & Almaiah, 2021). In the aviation and maritime sectors, coordinated monitoring, real-time threat analysis, network segmentation, and automated alerting mitigate cyber threats and protect critical operations (Ukwandu, et al., 2022; Abdelmagid et al., 2025). These examples demonstrate the practical application of resilience principles across diverse critical infrastructures.

A comprehensive approach to information security resilience is widely advocated, integrating proactive risk management, organizational governance, compliance and alignment with strategic objectives (Soomro et al., 2016; Grigaliūnas et al., 2024; Barbhuiya et al., 2024). Lessons from these critical infrastructure sectors offer valuable guidance for digitally intensive industries such as retail. Aligning cybersecurity frameworks such as ISO/IEC 27001 with core business goals enables risk prioritization, enhances customer trust, and strengthens overall competitiveness (Ardhaninggar & Ramli, 2024). As retailers adopt digital and omnichannel services, new vulnerabilities emerge, which can be mitigated through multi-layered security measures (Vaka, 2025; Symantec, 2024; Amosu et al., 2024).

Energy retail, with its complex digital operations, sensitive customer data, and diverse organizational cultures, can benefit from resilience principles from other critical infrastructures. Yet the sector remains underexplored, particularly regarding how resilience practices, critical controls, and cultural factors can address sector-specific risks and protect operations and data. This gap highlights a clear research need to advance information security resilience in European energy retail sector.

2.7 Conceptual synthesis

Information security resilience in the energy retail sector depends on integrated IT-GRC practices, which align organizational culture, standards, regulations, and critical controls with business objectives to mitigate sector-specific cybersecurity risks. Evidence from other critical infrastructures demonstrates that resilience emerges from proactive risk management, continuous situational awareness, sustained management engagement, and adaptive dynamic capabilities that allow organizations to adjust resources, processes, and strategies to evolving threats.

Despite extensive research in these sectors, energy retail remains comparatively underexplored, particularly regarding how cultural factors, the implementation and effectiveness of critical controls, and sector-specific risks interact to shape information security resilience, protect sensitive customer data, and maintain

operational continuity. This gap reflects the persistent disconnection between formal frameworks such as ISO/IEC 27001 and actual organizational practices, highlighting the need for empirically grounded, multidimensional approaches. Addressing this gap is critical for developing integrated resilience strategies that combine technical, procedural, and cultural dimensions, tailored to the unique challenges of the European energy retail sector.

3 MATERIALS AND METHODS

This dissertation adopts an inductive, exploratory, multi-method research design, combining qualitative and quantitative approaches across four embedded research papers. Here, "exploratory" refers to theory building and pattern identification grounded in empirical observation rather than hypothesis testing. Guided by an interpretivist philosophical stance, the study employs a case study design, survey research, and archival analysis to investigate information security challenges and practices within the European energy retail sector.

To integrate insights across cybersecurity culture, critical controls, and sector-specific risks, the dissertation adopts a typological approach as an analytical strategy for theory building. This approach systematically identifies patterns and categories that link governance mechanisms, human–technical interactions, and sector-specific cybersecurity challenges (Cornelissen, 2017; Leidner, 2020).

This approach enables the development of an empirically grounded structure, in which each paper contributes incrementally to theory building: Paper I identifies cultural dimensions, Papers II and III map critical control failures, and Paper IV synthesizes sector-specific risk patterns. Table 3 provides an overview of the methodological choices and analytical techniques applied in each paper, highlighting the multi-method, exploratory approach of this dissertation.

Table 3. Overview of methods and analytical techniques

Paper	Focus	Approach & philosophy	Design & time horizon	Data	Analysis
I	Cultural factors	Inductive, interpretivist	Single-case, cross-sectional (2023)	An 18-item employee survey sent to 2,100 employees (n = 610; response rate = 29%)	EFA
II & III	Critical controls / GDPR penalties	Inductive, interpretivist	Archival, cross-sectional (2020)	81 GDPR penalty cases (multi-industry, EU)	RCA, ISO/IEC 27001 mapping
IV	Key cybersecurity risks	Inductive, interpretivist	Single-case, longitudinal (2018–2023)	Internal cybersecurity incident reports	FMEA, bow-tie

Analytical techniques including Root Cause Analysis (RCA), Failure Modes and Effects Analysis (FMEA), bow-tie analysis, and Exploratory Factor Analysis (EFA) were employed to generate insights into cultural factors, failures, controls, and cybersecurity risks. The methodology of each paper is positioned according to Saunders et al.'s (2023) research onion framework, which provides a structured progression from the outermost layer of research philosophy, through approach, strategy, and time horizon, to the innermost layer of data collection and analytical

techniques. Figure 2 illustrates the research onion model as applied in this dissertation, showing how each layer informed the methodological decisions.

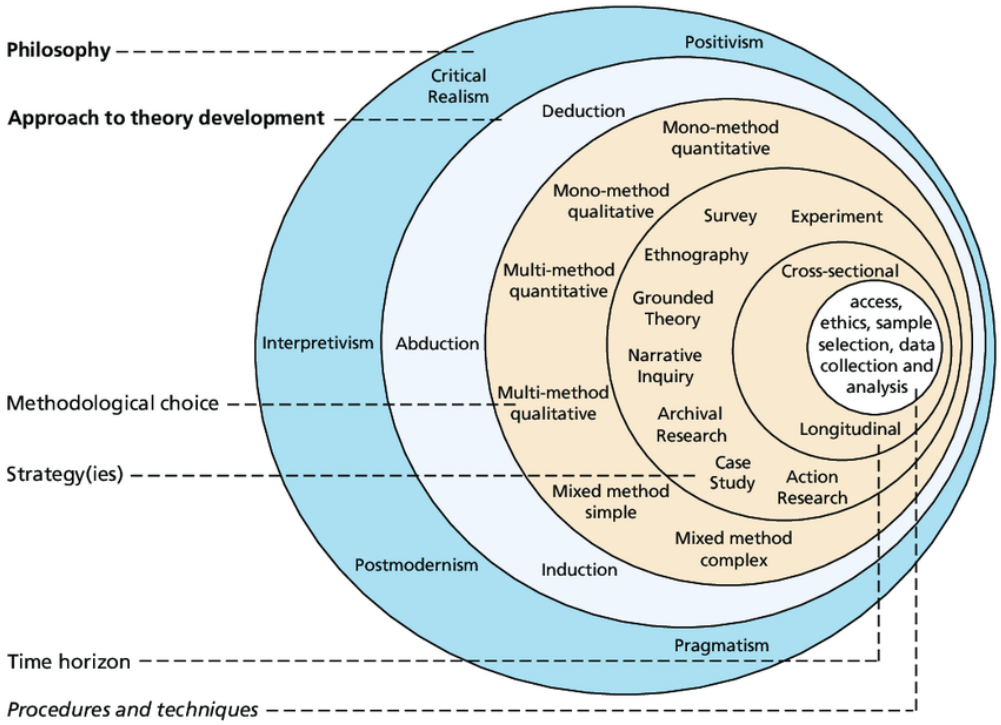

Figure 2. The research onion model

The chosen methods align with the dissertation's exploratory, inductive, and interpretivist orientation. Single-case and survey approaches enable in-depth examination of organizational phenomena, while archival and incident analyses provide insight into real-world information security failures and emerging risk patterns. Together, these complementary methods support systematic analysis of underlying causes, patterns, and relationships while remaining consistent with the overall research design. By integrating survey data, archival records, and incident reports, the multi-method approach enables triangulation, enhances methodological rigor, and contributes to a comprehensive understanding of information security within European energy retail organizations.

3.1 Paper I – cultural factors study

The cultural factors study applies Saunders et al.'s (2023) research onion to structure methodological choices from outermost to innermost layers. At the outermost layer, an interpretivist philosophy underpins the study, aiming to understand employee perceptions of information security within the organizational context. Within this interpretivist perspective, the focus is on understanding shared meanings,

perceptions, and socially constructed aspects of cybersecurity culture rather than establishing objective causal relationships. The second layer adopts an inductive approach, allowing insights to emerge from empirical data rather than testing predefined hypotheses, consistent with the exploratory focus.

At the strategy layer, a single-case study design was employed, focusing on a large European energy retail organization subject to the European Union's NIS2 Directive and GDPR. The organization operates across multiple European countries, supplying electricity and distributed energy resources (DERs), managing electric vehicle charging infrastructure, and maintaining an ISO/IEC 27001–aligned Information Security Management System (ISMS). The single-case design enabled in-depth examination of organizational context and culture, supporting rich interpretation of employee perceptions within a real-world operational environment.

At the innermost layer, data were collected through a quantitative survey aligned with the Cyber Security Culture Framework (Georgiadou et al., 2022) to systematically capture employee perceptions of information security culture. Although quantitative in format, the survey was used interpretively to explore shared perceptions and underlying cultural patterns rather than to test causal hypotheses. The survey was tailored to the organizational context and distributed via email to employees across relevant business units, with responses collected using Microsoft Forms. Participation was voluntary and anonymous, ensuring confidentiality and alignment with organizational data protection requirements. A cross-sectional time horizon was adopted, capturing perceptions at a single point in time in 2023.

The survey comprised 18 items, was sent to 2,100 employees, and was completed by 610 employees, yielding a 29% response rate. Exploratory Factor Analysis (EFA) was conducted on the survey data to identify latent dimensions of information security culture, reduce data complexity, and support the development of typologies of cultural drivers. Standard adequacy and reliability assessments were applied to ensure the suitability of the data for factor analysis and to support methodological rigor (Shrestha 2021; Howard, 2016). The cultural factors study contributes to the typology by identifying foundational dimensions of cybersecurity culture, forming the basis for integrating governance and human–technical interactions in subsequent papers.

3.2 Papers II and III – critical controls study

The critical controls study applies Saunders et al.'s (2023) research onion to structure methodological choices from outermost to innermost layers. At the outermost layer, an interpretivist philosophy underpins the study, aiming to understand context-

specific organizational failures and the mechanisms through which governance and compliance interact with operational practices. At the second layer, an inductive approach allows patterns and insights to emerge from empirical data rather than testing predefined hypotheses, consistent with the exploratory focus.

At the strategy layer, archival analysis was employed, examining 81 GDPR penalty enforcement cases from the year 2020 based on Article 32 ("security of processing"), sourced from the publicly available GDPR Enforcement Tracker maintained by CMS Law. This approach allowed the study to systematically investigate regulatory enforcement practices, organizational weaknesses, and patterns of control failures across multiple EU member countries and industries. At the time horizon layer, a cross-sectional design was applied, focusing on cases from a single year (2020) to provide a snapshot of compliance failures and associated control gaps.

At the data collection and analysis layers, each case was systematically mapped to ISO/IEC 27001 control-level failures using the supervisory authorities' published decisions as the authoritative record. Paper II applies the ISO/IEC 27001:2013 control set, while Paper III extends the analysis by remapping identified failures to the updated ISO/IEC 27001:2022 control structure, enabling examination of how revisions in controls and thematic restructuring affect the interpretation of critical control failures.

Quantitative techniques included frequency counts of control failures, cost estimation, and correlation analysis. Control failures were identified using ISO/IEC 27001 controls, enabling ranking by frequency, cost, and relationships. Root Cause Analysis (RCA) was used to determine underlying causes, connect them to specific controls, and examine interdependencies (Rooney, 2004). The resulting clusters formed typologies that integrated quantitative patterns with RCA insights, illustrating how governance, compliance, and operational practices interact to shape cybersecurity outcomes.

The combination of ISO/IEC 27001 control mapping, quantitative ranking, and RCA provided the basis for typologies that inform integration with cultural drivers (Paper I) and sector-specific risks (Paper IV). Extending the analysis to ISO/IEC 27001:2022 in Paper III ensures alignment with current standards. Although RCA is influenced by researcher assumptions (Peerally et al., 2017), coding and causal mapping were conducted systematically to reduce subjectivity and maintain consistency. Overall, archival analysis, quantitative mapping, and RCA offer a structured, typology-informed approach aligned with the exploratory and theory-building goals of the dissertation.

3.3 Paper IV – key risks study

The key risks study follows Saunders et al.'s (2023) research onion to structure methodological choices from outermost to innermost layers. At the outermost layer, an interpretivist philosophy underpins the study, with an exploratory focus on understanding cybersecurity risks and failures within a real-world organizational setting. The second layer adopts an inductive approach, allowing insights to emerge from actual cybersecurity incidents rather than testing predefined hypotheses.

At the strategy layer, a single-case design was employed, using the same case organisation from Paper I (cultural factors study) to ensure integration across typologies. At the time horizon layer, a longitudinal design was applied, analysing internally reported cybersecurity incidents over six years (2018–2023) to capture trends and emerging risks, following the best practices of case study design described by Eisenhardt (2007) and Yin (2018).

At the data collection and analysis layers, incidents were first categorized into eight key risk areas by the author, ensuring a consistent framework for analysis. Their underlying structures were then mapped to Failure Modes and Effects Analysis (FMEA), comprising a total of 21 failure modes, with tables independently populated by the author to ensure transparency and methodological rigor. To complement FMEA, bow-tie analysis was used as a graphical risk-modeling technique, demonstrating how threats, consequences, and controls can be visualized and managed (Meland et al., 2019; Bernsmed, 2018).

While FMEA and bow-tie analysis are inherently interpretive and may be influenced by researcher judgment, all categorizations and mappings were conducted systematically according to established procedures and guidelines (Carlson, 2012; Asllani et al., 2018). This structured approach captured the complex relationships among threats, consequences, and controls, enabling rigorous identification of risk patterns and maintaining both transparency and replicability across the analysis.

The analysis contributes to the development of a typology of cybersecurity risks, enabling structured integration with cultural drivers (Paper I) and critical controls (Papers II and III). Together, these typologies form a comprehensive, theory-informed framework for understanding organizational cybersecurity in European energy retail contexts.

3.4 Research ethics and data availability

Research ethics were addressed at the dissertation level to ensure consistency across all four papers. Paper I involved direct data collection from human participants via an internal organizational survey. Survey participation was voluntary, the organization was anonymized, and no personal or demographic data were collected, minimizing the risk of respondent identification.

Papers II and III used publicly available GDPR enforcement data, while Paper IV analyzed internally reported cybersecurity incidents from the same case organization as Paper I. All data were handled in anonymized form and within established organizational information security, compliance, and research governance practices. No sensitive personal data or vulnerable populations were involved.

All studies were conducted in accordance with German and EU regulations, including GDPR, and institutional guidelines for organizational research. Because data were anonymized, publicly available, or securely handled internally, formal review by a university ethics committee was not required. Detailed descriptions of data collection and analysis ensure transparency and support the drawing of general insights, rather than making statistical claims about populations.

4 RESULTS AND DISCUSSION

This section presents how the results of each of the three main research questions, along with their sub-questions, are addressed across the four research papers. Collectively, these insights provide an integrated empirical analysis of cultural factors, critical controls, and organizational risks that inform decisions to strengthen information security resilience in the critical context of the European energy retail sector.

4.1 Factors of a resilient information security culture

Paper I examined the factors of information security culture through a survey-based analysis of 18 security culture items within a European energy retail organization. The survey captured multiple dimensions of information security culture, including risk perception, awareness, policy compliance, management commitment, responsibility, reporting practices, trust, teamwork, performance assessment, and security-related behaviors. Together, these dimensions provided a comprehensive perspective on employees' engagement with information security.

Table 4. Results of Paper I

RQ	Sub-RQ	Results
RQ1: What are the key factors that drive the strengthening of information security culture in energy retail organizations?	-	Analysis of survey responses identified three key factors, each with two subcomponents: 1. Management engagement in information security: top management commitment; direct management engagement. 2. Assessment and recognition of information security performance: inclusion in performance evaluations; recognition and rewards. 3. Assignment of responsibility for information security reporting: responsibility for risk reporting; responsibility for incident reporting.

Exploratory Factor Analysis (EFA) identified three key factors, each consisting of two subcomponents, reflecting the underlying structural dimensions of information security culture. Table 4 summarizes the results.

1. Management engagement in information security

- Top management commitment: Senior leadership sets strategic direction, prioritizes security, and allocates necessary resources.

- Direct management engagement: Managers amplify the voice of top management, implement policies in daily operations, and reinforce security expectations at the team level.

2. Assessment and recognition of information security performance

- Inclusion in performance evaluations: Security responsibilities are integrated into ongoing performance management, supporting accountability and attention to secure practices.

- Recognition and rewards: Positive security behaviors are systematically acknowledged to reinforce consistent adherence to security practices.

3. Assignment of responsibility for information security reporting

- Responsibility for risk reporting: Employees are responsible for identifying and reporting potential risks to information, supporting overall security and operational effectiveness.

- Responsibility for incident reporting: Employees are responsible for promptly reporting security incidents to enable mitigation, learning, and organizational resilience.

Collectively, these factors demonstrate that leadership support, accountability, recognition, and structured reporting are central to promoting a resilient information security culture. They align organizational objectives with employee behavior, awareness, and engagement, thereby enhancing the organization's ability to manage information security risks effectively.

4.2 Critical controls for common cybersecurity gaps

Papers II and III analyzed information security failures across European organizations in multiple industry sectors, identifying the most frequent and costly failures, their correlations, sector-specific differences, and mappings to ISO/IEC 27001:2013 and ISO/IEC 27001:2022 controls.

ISO/IEC 27001:2013 structures its requirements hierarchically. Individual controls are grouped under broader control objectives, which are in turn organized into control clauses representing specific domains of the standard. This hierarchy allows reporting and analysis at multiple levels, from specific operational failures to overarching management requirements. ISO/IEC 27001:2022 simplifies the structure by consolidating controls into four thematic groups, removing the previous control objectives and clause hierarchy.

Table 5 summarizes the key findings from Papers II and III. The synthesis of these cases shows that failures in information access controls, system change management,

information classification, employee awareness education and training, privileged access management, system security testing, malware protection, and the secure handling of physical and electronic assets are the most frequent and financially significant. Prioritizing these areas can strengthen organizational resilience against both recurring and high-impact information security risks in European energy retail organizations.

Table 5. Results of papers II and III

RQ	Sub-RQ	Results
RQ2: What are the most frequent and most expensive information security failures corresponding to ISO 27001 controls?	-	Analysis of GDPR penalty cases identified a core set of critical controls: information access controls, system change management, information classification, employee awareness education and training, privileged access management, system security testing, malware protection, and the secure handling of physical and electronic assets, which are the most frequent and financially significant.
-	RQ2.1: How many information security failures corresponding to ISO 27001 controls typically exist in a GDPR penalty case?	The number of information security failures per case ranges from 1 to 13, with most cases involving a small number of failures. Two or three failures account for the majority of cases, while cases with more than ten failures are rare but associated with exceptionally high penalties.
-	RQ2.2: How do the information security failures corresponding to ISO 27001 controls correlate?	Strong correlations were observed among specific controls, indicating that certain failures tend to co-occur. Notable links include working in secure areas and information labeling, physical media transfer and the management of removable media, change management and the management of privileged access rights, as well as end-to-end event reporting and incident-handling procedures.
-	RQ2.3: Are there any industry type differences in information security failures and penalties?	Both the frequency and financial severity of information security failures vary substantially across industry sectors. Some sectors exhibit high numbers of cases with low penalties, while others show fewer cases with significantly higher average penalties.
-	RQ2.4: What are the most frequent and most expensive information security failures corresponding to ISO/IEC 27001:2022 controls, and what is their correlation?	Mapping to ISO/IEC 27001:2022 confirms that the most frequent and costly failures largely mirror those identified under the 2013 standard, highlighting access management, information classification, change management, system testing, employee awareness, and incident management as typical shortcomings.

In response to RQ2, the analysis of GDPR penalty cases identifies the most critical control-level information security failures.

- Information access restriction: The most frequent shortcomings were observed in access control management, resulting in excessive access rights, increased risk of unauthorized data disclosure, modification, or loss, and high-impact security incidents.

- Change management controls: The most costly weaknesses were observed in change management processes, which can result in loss of oversight of information systems and severe data inconsistencies. Even infrequent occurrences can have disproportionate financial impacts, highlighting the need for resilient operational procedures.

- Classification of information: Highly frequent and financially significant shortcomings reflect challenges in organizational risk assessment frameworks. Without comprehensive implementation of this control, there is insufficient insight into risk levels and the need to implement further risk-based controls.

- Information security awareness, education and training: Very frequent and moderately costly human-factor limitations highlight the need for targeted awareness campaigns to ensure policy adherence and a security-conscious culture.

- Management of privileged access rights: Very costly and moderately frequent failings in assigning and monitoring privileged accounts can lead to unauthorized system access, data compromise, and significant financial and operational impacts.

- System security testing: Costly and frequent shortcomings in testing information system vulnerabilities highlight persistent weaknesses in operational procedures and the need for strengthened oversight.

- Electronic messaging: Frequent deficiencies in handling electronic messages, including improper use, storage, and transmission, increase the risk of data leakage, unauthorized access, and operational disruptions.

- Handling of assets: Frequent shortcomings in the secure transport of physical media indicate inadequate protection of information assets from loss, unauthorized access, or misuse.

- Policy on the use of cryptographic controls: Frequent shortcomings were observed in applying cryptographic policy, specifically in encrypting electronic messages and physical media during transport, which increases the risk of data breaches and unauthorized access.

- Controls against malware: Less frequent but financially significant weaknesses in malware prevention highlight the need for strengthened security measures throughout the system lifecycle.

In response to RQ2.1, analysis of GDPR penalty cases shows that the number of information security failures ranges from one to thirteen per case. Most cases involve a low number of failures: 30% had two failures, 25% had three, and 12% had a single failure. Cases with four or more failures accounted for 33% of all cases. Notably, only two cases had more than ten failures, with the case recording the highest number, thirteen failures, incurring a penalty of over €22 million.

In response to RQ2.2, correlations among information security failures were analyzed. The strongest correlations highlight which control-level shortcomings tend to co-occur across cases, providing insights into clusters of related failures that may increase organizational risk. These patterns do not imply causation but suggest that addressing linked controls may help prevent multiple simultaneous security weaknesses.

- Working in secure areas ↔ Labeling of information (correlation 1.00): This perfect positive correlation indicates that lapses in physical security always coincide with improper information labeling and mishandling of sensitive information. Several cases involved employees disposing of sensitive documents in unsecured trash bins outside the organization, resulting in confidentiality breaches when outsiders accessed the discarded materials.

- Physical media transfer ↔ Management of removable media (correlation 0.81) & Review of policies for information security (correlation 0.70): These strong positive correlations suggest that failures in transferring physical media frequently occur alongside inadequate removable media management and insufficient policy review. In many cases, unencrypted removable media were lost or stolen, creating a heightened risk of unauthorized data access.

- Change management ↔ Management of privileged access rights (correlation 0.70) & Controls against malware (correlation 0.70): These strong positive correlations highlight that weaknesses in change management frequently occur alongside mismanaged privileged accounts and outdated malware controls. Such failures could cascade into unauthorized changes, unauthorized access or privilege escalation, and increased vulnerabilities.

- Reporting information security events ↔ Responsibilities and procedures (correlation 0.65): This strong positive correlation suggests that failures in reporting information security events often occur alongside unclear processes and poorly defined responsibilities, raising the likelihood of delayed or inadequate incident response.

- Assessment and decision on information security events ↔ Response to information security incidents (strong correlation 0.65): This strong positive correlation shows that deficiencies in assessing and deciding on information security events often occur alongside shortcomings in incident response, allowing incidents to escalate in severity and impact.

In response to RQ2.3, analysis of GDPR penalties in 2020 reveals substantial variation in both the number and financial impact of information security failures across industry sectors. A total of 81 Article 32 penalties, amounting to nearly €100 million, were issued for insufficient technical and organizational security measures, with an overall average of €1,220,411 per case.

The Media, Telecoms, and Broadcasting sector received the highest total penalties (€42,050,136 across 17 cases, averaging €2,473,537 per case). In contrast, the Public Sector and Education sector also had 17 cases, but with a much lower total (€1,606,300, averaging €94,488 per case), reflecting differences between industries. Sectors with the highest average penalties included Accommodation and Hospitality (€20,450,000 for a single case) and Transportation and Energy (€4,412,000 across five cases), whereas Real Estate and Employment incurred the smallest penalties. These findings indicate that both the frequency and financial severity of information security failures are highly industry-dependent, underscoring the need for sector-specific risk management and compliance strategies.

Finally, analysis mapped to ISO/IEC 27001:2022 controls (RQ2.4) confirms that the most frequent and costly failures largely mirror those identified under the 2013 standard. The results highlight a core set of technical, organizational, and human-related controls, particularly access management, information classification, change management, system testing, employee awareness, and incident management, which drive both the frequency and financial impact of failures. Addressing these controls and their correlated areas can substantially reduce risk exposure and strengthen resilience in European energy retail organizations.

4.3 Key information security risks in energy retail

Paper IV examined cybersecurity risks in the European energy retail sector through a structured analysis of incidents and their associated risk categories. Using Failure Mode and Effects Analysis (FMEA) and graphical attack modeling, the study provides a systematic view of how technical, organizational, and human-related risks manifest and how they can be mitigated. Table 6 summarizes the results.

Table 6. Results of paper IV

RQ	Sub-RQ	Results
RQ3: What are the main cybersecurity risk categories for the energy retail business?		Eight key cybersecurity risk categories were identified: (1) socially engineered phishing; (2) cyberattacks; (3) change management; (4) access control; (5) insider threats; (6) data protection compliance; (7) supply chain security; and (8) physical security.
-	RQ3.1: What are the cybersecurity failure modes, effects, and corresponding mitigation measures for the energy retail business?	The FMEA of each risk subcategory identified a total of 21 failure modes, along with their effects, causes, and controls, showing that risks arise from human, process, and technical interactions. Layered preventive and detective measures are key to reducing their likelihood and impact.
-	RQ3.2: How can graphical attack modeling techniques enhance cybersecurity risk management for the energy retail business?	Bowtie modeling of phishing and unauthorized access scenarios illustrates attack paths, controls, and consequences, exemplifying complex defenses and highlighting critical controls for prioritization.

In response to RQ3, analysis identified eight key cybersecurity risk categories relevant to the energy retail business. These categories reflect recurring risk themes observed across operations, systems, and human activities. The identified risk categories are as follows:

1. Lack of resilience against socially engineered phishing attacks: Weak employee awareness, insufficient reporting practices, and limited protection against socially engineered phishing enable credential theft, malware infections, and financial fraud.

2. Insufficient resilience of information systems against cyberattacks: Unaddressed vulnerabilities, exposed services, and insufficient defenses increase susceptibility to cyberattacks, including denial-of-service, brute-force, injection, and ransomware attacks.

3. Weak change management controls: Insufficient approval, testing, and post-implementation controls create system instability and opportunities for exploitation during changes.

4. Inadequate access control management: Weak enforcement of access policies and poor privileged access management increase the risk of unauthorized access and data compromise.

5. Insider threat risk: Limited risk assessments increase the likelihood of intentional or accidental misuse by trusted users.

6. Insufficient data protection compliance: Deficiencies in privacy governance, contract handling, and data processing practices increase the risk of regulatory noncompliance and financial penalties.

7. Supply chain risk: Inadequate asset management and insufficient supplier oversight introduce significant third-party risks, increasing exposure to vulnerabilities, data breaches, and operational disruptions.

8. Deficient physical security management: Unauthorized access, theft, and aggressive behavior toward staff members threaten both information confidentiality and personal safety.

In response to RQ3.1, a total of 21 subcategories across eight risk categories were analyzed using FMEA to identify typical failure modes, their potential effects, underlying causes, and corresponding prevention and detection measures. Together, these results demonstrate that cybersecurity risks in the energy retail sector emerge from the interaction of human behavior, process weaknesses, and technical deficiencies. FMEA underscores the importance of layered preventive and detective controls to reduce both the likelihood and impact of these risks.

To address RQ3.2, bowtie modeling was used to exemplify the visualization of representative risk scenarios based on two selected FMEA subcategories: phishing attacks and unauthorized physical access. The methodology of the bowtie model, along with the corresponding visualizations, is presented in Paper IV of this dissertation. These models depict attack paths, preventive and detective barriers, and potential consequences, illustrating how multiple layers of control interact to prevent escalation. The results show that bowtie models complement FMEA and risk communication by making complex attack–defense relationships explicit and by highlighting critical controls that require prioritization.

In the bowtie-illustrated phishing attack scenario, the attacker seeks to acquire privileged user credentials and install malware. While generic phishing attempts may be blocked by spam filters, targeted social engineering attacks can bypass these controls. Preventive measures include user awareness training, phishing simulations, and multi-factor authentication. Detection controls, such as behavioral analytics and endpoint security, mitigate risk by reducing credential misuse and malware execution. The model demonstrates how technical and human-focused defenses interact to prevent attack escalation while accounting for potential attacker adaptations.

In another visualized example, the unauthorized physical access scenario, the attacker attempts to enter secure areas without proper credentials, by tailgating or

stealing access cards. Defenses include ID badge policies, staff vigilance training, mantraps, strong authentication at entry points, surveillance systems, guards, clean desk policies, and secure zones. The bowtie model illustrates how multiple layers of procedural, technical, and human controls reduce both the likelihood and impact of such attacks, even if individual controls are bypassed.

Collectively, the findings of Paper IV extend the results of previous papers by translating identified control weaknesses and human factors into concrete risk scenarios. The combined use of risk categorization, FMEA, and bowtie visualization provides a coherent framework for understanding, communicating, and managing cybersecurity risks in the European energy retail sector.

4.4 Discussion

The findings indicate that strengthening information security resilience in the European energy retail sector requires a comprehensive, multi-layered approach. Culture and governance act as foundational drivers, where leadership engagement, accountability, and clear reporting responsibilities shape behavior and reinforce adherence to security practices. Leadership commitment and active management communication support embedding security into daily operations, while recognition and performance assessment encourage proactive participation by staff. Reporting mechanisms ensure timely identification and mitigation of risks, strengthening organizational vigilance.

Technical, human, and process-related failures tend to cluster in key areas, including weak access controls and privileged access management, deficiencies in system change management, malware protection, and security testing, as well as risk-based information classification and employee awareness and training. They also occur in the secure handling of physical and electronic assets and in end-to-end reporting and incident handling procedures. These failures often interact, compounding one another and creating cascading risks. For example, weak change management combined with poorly monitored privileged access in information systems can significantly increase both the likelihood and impact of cyber incidents. While most failures are limited in scope, rare incidents can result in significant financial, operational, and regulatory consequences, highlighting the need for a proactive risk management approach.

Structured assessment methods, such as FMEA, provide a systematic view of failure modes, their potential effects, and corresponding preventive and detective controls across eight key risk categories, from socially engineered phishing to physical security. FMEA emphasizes the importance of layered controls, illustrating that

mitigating human, process, and technical vulnerabilities in isolation is insufficient. Bowtie modeling complements this approach by visualizing attack paths, control barriers, and potential consequences, making complex attack–defense interactions explicit and understandable. These visualizations support prioritization, resource allocation, and risk communication, enabling decision-makers to focus on the most critical controls while maintaining a clear understanding of residual risks.

Collectively, these findings underscore that resilient information security depends on the coordinated interplay of leadership, culture, human vigilance, and procedural and technical controls. Embedding a resilient security culture enhances awareness and reporting behaviours, while structured tools and visualizations provide clarity and actionable guidance. The integration of these elements creates a dynamic, adaptive defense posture capable of addressing both common operational failures and high-impact, low-probability incidents.

Furthermore, the results highlight the value of sector-specific approaches. The energy retail context, with its complex IT interfaces and organizational processes, regulatory obligations, and reliance on third-party suppliers, presents unique vulnerabilities that require tailored risk assessment and mitigation strategies. Aligning cultural, organizational, and technical measures ensures that controls are not only compliant but also operationally effective, enhancing resilience in a rapidly evolving threat landscape.

5 CONCLUSIONS

This chapter synthesizes the key findings, contributions, and implications of the dissertation. Drawing on four empirical studies, it offers a comprehensive perspective on information security resilience in the European energy retail sector. The analysis focuses on organizational culture, compliance failures, critical controls, and sector-specific cybersecurity risks. By integrating these insights, the chapter highlights both theoretical and managerial relevance. It concludes by discussing limitations and proposing directions for future research to advance knowledge and strengthen the security of energy retail operations.

5.1 Thesis statement

This dissertation demonstrates that strengthening information security resilience in the European energy retail sector requires a comprehensive approach that integrates cultural factors, critical controls, and key risks. While frameworks such as ISO/IEC 27001 provide structural guidance, recurring failures often stem from limited reinforcement of security culture and shortcomings in control implementation and risk management. The findings indicate that information security resilience depends on combining technical safeguards with engaged leadership, clear accountability, and a shared organizational understanding of cybersecurity responsibilities. This approach is supported by systematic tools, such as FMEA and bowtie modeling, which help map, visualize, and mitigate risks across technical, human, and process domains.

5.2 Key findings

The results of Paper I show that a resilient information security culture in European energy retail organizations is shaped by three core factors: management engagement, assessment and recognition of security performance, and clearly assigned responsibility for security reporting. Executive commitment and direct managerial engagement embed security into daily work practices, while integrating security responsibilities into performance evaluations and recognizing positive behavior strengthens accountability and encourages proactive participation. Clearly defined responsibilities for risk and incident reporting further support early detection, learning, and continuous improvement, reinforcing organizational resilience.

Findings from Papers II and III identify a concentrated set of information security weaknesses that drive both the frequency and financial severity of GDPR penalties. The most critical failures include information access controls, privileged access management, system change management and security testing, malware protection,

risk-based information classification, employee awareness and training, the secure handling of physical and electronic assets, and end-to-end event reporting and incident handling procedures. Although most cases involve only a few failures, rare incidents with multiple, correlated control breakdowns result in exceptionally high penalties. Strong correlations among specific controls indicate that failures frequently co-occur, highlighting the importance of addressing clustered controls collectively rather than in isolation.

Paper IV translates these control weaknesses and human factors into concrete cybersecurity risk categories specific to the energy retail sector. Eight principal risk categories were identified, spanning technical, organizational, and human-related risks, including socially engineered phishing, cyberattacks, change management, access control, insider threats, data protection compliance, supply chain security, and physical security. Using FMEA and bowtie modeling, the study demonstrates that cybersecurity risks emerge from the interaction of people, processes, and technology. Layered preventive and detective controls reduce both the likelihood and impact of these risks, while graphical attack modeling improves risk communication and supports prioritization of the most critical controls.

Table 7. Key findings and implications

Paper(s)	Focus	Key findings	Energy retail implications
Paper I	Information security culture	A resilient security culture is driven by management engagement, assessment and recognition of security performance, and clear accountability for security reporting. Leadership participation embeds security into daily work, while performance-linked responsibilities and recognition motivate proactive behavior.	Strengthening leadership commitment, formal accountability, and recognition mechanisms enhances early detection, organizational learning, and overall resilience.
Papers II & III	GDPR penalties and control failures	A core set of control failures drives the frequency and severity of penalties. Key deficiencies include weak access controls, privileged access management, gaps in system change management, malware protection, security testing, risk-based information classification, and employee training. Failures also occur in handling physical and electronic assets and in end-to-end reporting. While most penalties involve few failures, correlated breakdowns can trigger exceptionally high fines.	Addressing the core set of controls is essential, as isolated fixes are insufficient when control failures co-occur and amplify risk.
Paper IV	Cybersecurity risks and modeling	Eight sector-specific risk categories were identified: phishing attacks, cyberattacks, weak change management, inadequate access controls, insider threats, insufficient data protection compliance, and supply chain and physical security vulnerabilities. These risks arise from interactions among people, processes, and technology. Layered controls, combined with graphical attack modeling, enhance mitigation and improve risk communication.	Structured risk categorization and visual modeling support prioritization, clearer communication, and more effective deployment of preventive and detective controls.

Table 7 summarizes the key findings across all four papers, integrating cultural, control-related, and risk-modeling perspectives. This synthesis provides a unified view of how leadership, accountability, technical controls, human factors, and structured risk management collectively support the strengthening of information security practices in European energy retail organizations.

5.3 Theoretical contribution

The academic literature recognizes multiple forms of theoretical contribution, including typologies, process narratives, and integrative frameworks (Cornelissen, 2017; Leidner, 2020). This dissertation provides both typological and integrative contributions by linking culture, controls, and sector-specific risks. Paper I advances theory on cybersecurity culture, while Papers II, III, and IV provide empirical evidence on critical controls, recurring patterns, and sector-specific risks, collectively supporting a unified understanding of information security resilience in European energy retail organizations.

By conceptualizing cybersecurity culture as a governance-mediated process, this study addresses gaps identified by Gcaza & von Solms (2017) and Uchendu et al. (2021). Rather than treating culture as an abstract phenomenon, it demonstrates how IT-GRC and structured control practices actively shape and reinforce it. Expanding on prior work emphasizing management commitment (Vincent et al., 2019), the study highlights the role of structured incident and risk reporting (Ahola et al., 2025), integrating security responsibilities into performance assessments (Gravina et al., 2021), and recognizing compliant behavior (Vuong & Nguyen, 2022). While accountability and reporting are typically explored in management literature rather than culture studies (Pearson & Sutherland, 2017; Li et al., 2024), this study extends the view to energy retail, drawing on evidence from high-reliability sectors such as nuclear safety (Ilina & Sundquist, 2012) and aviation (Rodrigues & Filho, 2025).

The dissertation also bridges the gap between regulation and practice, as highlighted by Dlamini et al. (2009), by examining how regulation shapes organizational IT-GRC practices. Analysis of GDPR penalty cases extends prior research (Akhlaghpour et al., 2021; Presthus & Sønslien, 2021; Ruohonen & Hjerppe, 2022) by linking reported failures to ISO/IEC 27001 controls and identifying the most critical ones. These findings provide an updated, evidence-based perspective on organizational information security implementation, addressing the need highlighted by Vaibhav (2022) and aligning with prior studies (Khajouei et al., 2017; Shojaie et al., 2014). Building on Leidner's (2020) notion of integrative contribution, the study introduces

a novel method to analyze GDPR penalty case reports, map failures to ISO/IEC 27001 controls, and rank the most critical ones. This analysis further informs the typology by linking specific control failures to broader cultural and risk patterns.

Finally, the dissertation addresses a notable gap in cybersecurity research on the energy retail sector, which faces complex IT infrastructures, large volumes of customer data (Nazari & Musilek, 2023), stringent regulatory requirements (Gerber & von Solms, 2008), and significant cyber threats (Falowo et al., 2022). While prior studies in the energy industry focus on power generation, grid operations, broader energy value chains, or customer-facing DER solutions (Bıçakcı & Evren, 2023; Lee et al., 2023; Wang & Lu, 2013; Sun et al., 2018; Gong & Lee, 2021; Nikolaou et al., 2023; Zografopoulos et al., 2023), this dissertation integrates insights from culture, critical controls, and sector-specific risks to provide an empirically informed framework for energy retail. It offers practical guidance for IT-GRC decision-making, including an enhanced understanding of complex risks through attack–defense visualizations, as highlighted by Staheli et al. (2014) and de Ruijter and Guldenmund (2016).

5.4 Managerial implications

The following actions provide a structured, layered approach for managers and practitioners to enhance information security resilience by strengthening culture, prioritizing critical controls, and managing key cybersecurity risks.

1. Engagement across leadership and teams: Provide clear direction and ensure security priorities are adequately resourced at the executive level. Communicate and reinforce these priorities at the team level to drive awareness, policy adherence, and vigilance through targeted support and appointed cybersecurity champions.

2. Performance management and accountability: Integrate security responsibilities, recognition of compliant behavior, and accountability for risk and incident reporting into performance management processes, ensuring that members of staff at all levels understand their roles, consistently follow policies, and contribute to maintaining a strengthened security posture.

3. Key control verification: Prioritize the most critical controls, including least-privilege access and the review, audit, and control of privileged accounts, to mitigate the risk of unauthorized access. Ensure traceable change management procedures, malware controls, security testing, and event

monitoring and logging are established to facilitate secure system lifecycle management.

4. Assurance of clustered controls: Identify and reinforce interdependent controls to prevent cascading risks, and prioritize systematic information classification to ensure risk-based control implementation across an information asset landscape that is kept continuously up-to-date. Establish and enforce policies for the secure handling of physical and electronic information through targeted awareness programs. Implement comprehensive incident management procedures encompassing reporting, assessment, response, and resolution.

5. Management of key cybersecurity risk areas: Address high-priority risks, including socially engineered phishing, cyberattacks such as ransomware, denial-of-service, and injection attacks, weaknesses in change management and access controls, insider threats, data protection compliance, supply chain vulnerabilities, and physical security. Conduct a systematic analysis of each area to identify potential failure modes and select appropriate countermeasures for mitigation.

6. Visualized risk analysis: Perform an in-depth visual attack–defense analysis of selected high-priority risks to communicate them effectively across departments and to executives, supporting risk-based and strategic decision-making. Integrate technical, procedural, and human-focused measures into a layered defense approach that informs these decisions.

5.5 Limitations and future research

While this dissertation offers key insights into information security resilience, culture, critical controls, and risks, the generalizability of the findings is shaped by methodological and contextual factors, in line with broader discussions on research generalization (Lee & Baskerville, 2003). The results may be cautiously transferable to large European energy retail organizations and similarly regulated critical sectors with comparable governance structures, regulatory environments, and cybersecurity challenges. The following considerations outline key boundaries of applicability and directions for future research within IT-GRC contexts.

The culture study focuses on a single European energy retail organization, which may limit applicability across varying organizational cultures, regulatory settings, and levels of security maturity. The cross-sectional design captures culture at a single point in time, and reliance on self-reported survey data may introduce response bias.

In addition, using exploratory factor analysis with orthogonal varimax rotation simplifies interpretation but may obscure interdependencies among cultural drivers. Future research could incorporate longitudinal and multi-organizational datasets to examine cultural evolution and contextual variation. Studies could also explore the role of team-level cybersecurity champions in translating policy into practice and investigate how mature safety-critical sectors, such as nuclear and aviation, develop transferable security culture practices.

The critical controls analysis relies on GDPR penalty reports whose quality and detail vary across EU supervisory authorities, and enforcement datasets may be incomplete or influenced by ongoing appeals. Penalty decisions are often holistic, limiting precise attribution to specific violations, and root cause analysis introduces interpretive subjectivity. Future research could conduct comparative cross-industry studies, longitudinal analyses of enforcement trends, and apply complementary analytical approaches such as automated text mining or machine learning to enhance objectivity and identify emerging failure patterns.

The key risks study draws on formally reported incidents, which may exclude undetected events and affect completeness. Qualitative FMEA assessment introduces interpretive judgment, and findings are influenced by organization-specific context and the evolving nature of cyber threats. Expanding research to multiple organizations, applying standardized modeling approaches, and further examining interactions among technical, procedural, and human controls would strengthen generalizability and refine typologies linking culture, controls, and sector-specific risks.

Finally, this dissertation advocates structured, typology-informed research that links organizational culture, critical controls, and sector-specific cybersecurity risks within IT-GRC–driven ISMS environments. These integrative approaches close gaps between policy and practice, enhance risk understanding, guide investment priorities, and strengthen resilience against cyber threats while ensuring compliance with evolving regulations. Beyond providing actionable guidance for energy retail organizations, the study calls for further research to advance empirically grounded, sector-specific cybersecurity practices across this sector and other critical infrastructure industries.

References

Abdelmagid, A. M., Javadnejad, F., Pinto, C. A., & Diaz, R. (2025). A new cyber risk identification and assessment approach of the maritime cyber risks. *Enterprise Information Systems, 19*(1), 1–23. https://doi.org/10.1080/17517575.2025.2524848

Adeyinka, A. V., Moronkunbi, M. A., Oyedeji, O. C., Olusegun, P. V., & Samuel, S. A. (2024). The role of IT governance, risk, and compliance (IT GRC) in modern organizations. *International Journal of Latest Technology in Engineering, Management and Applied Science, 13*(6), 44–50. https://doi.org/10.51583/IJLTEMAS.2024.130607

Afzal, Z., Ekstedt, M., Müller, N., & Mukherjee, P. (2024). Security challenges in energy flexibility markets: A threat modelling-based cyber security analysis. *Electronics, 13*(22), 4522. https://doi.org/10.3390/electronics13224522

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity, 4*(1), tyy006. https://doi.org/10.1093/cybsec/tyy006

Ahola, K., Butavicius, M., McCormac, A., & Sturman, D. (2025). Hey "CSIRI", should I report this? Investigating the factors that influence employees to report cyber security incidents in the workplace. *Information and Computer Security, 33*(2), 242–266. https://doi.org/10.1108/ICS-11-2023-0214

Akhlaghpour, S., Hassandoust, F., Fatehi, F., Burton-Jones, A., & Hynd, A. (2021). Learning from enforcement cases to manage GDPR risks. *MIS Quarterly Executive, 20*(3), 199–218. https://doi.org/10.17705/2msqe.00049

Alam, S. E., & Shukla, D. (2022). Optimal regulation of prosumers and consumers in smart energy communities. In *2022 IEEE International Smart Cities Conference (ISC2)* (pp. 1–6). IEEE. https://doi.org/10.1109/ISC255366.2022.9921890

AlHogail, A., & Mirza, A. (2014). Information security culture: A definition and a literature review. In *2014 World Congress on Computer Applications and Information Systems (WCCAIS)* (pp. 1–7). IEEE. https://doi.org/10.1109/WCCAIS.2014.6916579

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior, 49*, 567–575. https://doi.org/10.1016/j.chb.2015.03.054

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences, 11*(8), 3383. https://doi.org/10.3390/app11083383

Aljohani, T. M. (2024). Cyberattacks on energy infrastructures as modern war weapons – Part II: Gaps, standardization, and mitigation. *IEEE Technology and Society Magazine, 43*(2), 70–77. https://doi.org/10.1109/MTS.2024.3395697

Al-Mhiqani, M. N., Rabiah, A., Zaheera, Z. A., Warusia, M., Aslinda, H., & Clarke, N. L. (2018). A new taxonomy of insider threats: An initial step in understanding authorised attack. *International Journal of Information Systems and Management, 1*(4), 343–359. https://doi.org/10.1504/IJISAM.2018.094777

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

Alnatheer, M. A. (2015). Information security culture critical success factors. In *2015 12th International Conference on Information Technology – New Generations* (pp. 731–735). IEEE. https://doi.org/10.1109/ITNG.2015.124

Amosu, O. R., Kumar, P., Ogunsuji, Y. M., Adelaja, A., Faworaja, O., & Adetula, K. (2024). Enhanced cybersecurity measures: Protecting customer data in the e-commerce and retail industry. *World Journal of Advanced Research and Reviews, 23*(2), 890–900. https://doi.org/10.30574/wjarr.2024.23.2.2408

Anass, R., Assoul, S., Ouazzani Toure, K., & Roudies, O. (2020). Information and cyber security maturity models: A systematic literature review. *Information and Computer Security, 28*(4), 627–644. https://doi.org/10.1108/ICS-03-2019-0039

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). IEEE. https://doi.org/10.1109/ACEPT.2017.8168583

Ani, U. P. D., He, H. (Mary), & 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

Ardhaninggar, E. A., & Ramli, K. (2024). A review of cybersecurity framework implementation for the retail industry: Challenges and recommendations. *ARRUS Journal of Engineering and Technology, 4*(2), 211–219. https://doi.org/10.35877/jetech3434

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*, e268. https://doi.org/10.1002/wene.268

Barbhuiya, I. A., Laroiya, S., & Singh, R. (2024). Holistic cybersecurity risk management framework. *SSRN*. https://doi.org/10.2139/ssrn.4759581

Barrett, C. (2020). Emerging trends from the first year of EU GDPR enforcement. *Scitech Lawyer, 16*(3), 22–25, 35.

Beckel, C., Sadamori, L., Staake, T., & Santini, S. (2014). Revealing household characteristics from smart meter data. *Energy, 78*, 397–410. https://doi.org/10.1016/j.energy.2014.10.025

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. Stølen (Eds.), *Graphical models for security: GraMSec 2017* (Lecture Notes in Computer Science, Vol. 10744, pp. 43–60). Springer, Cham. 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

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience – Fundamentals for a definition. In A. Rocha, A. Correia, S. Costanzo, & L. Reis (Eds.), *New contributions in information systems and technologies* (Advances in Intelligent Systems and Computing, Vol. 353, pp. 323–334). Springer, Cham. https://doi.org/10.1007/978-3-319-16486-1_31

Björnsdóttir, S., Jónsson, P., de Boer, R., & Thorsteinsson, S. (2022). The importance of risk management: What is missing in ISO standards? *Risk Analysis, 42.* https://doi.org/10.1111/risa.13803

Brenner, J. (2007). ISO 27001 risk management and compliance. *Risk Management, 54*(24), 26, 28–29.

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. https://doi.org/10.1016/B978-0-12-816835-6.00001-2

Burger, M., Graeber, B., & Schindlmayr, G. (2014). Managing energy risk: An integrated view on power and other energy markets. John Wiley & Sons.

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

Choubey, S., & Bhargava, A. (2018). Significance of ISO/IEC 27001 in the implementation of governance, risk and compliance. *International Journal of Scientific Research in Network Security and Communication, 6*(2), 30–33.

CMS Law. (2022). *GDPR enforcement tracker – The Netherlands: Fine against Uber (ETid-1005)*. Enforcement Tracker. Retrieved September 23, 2025, from https://www.enforcementtracker.com/ETid-1005

Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows. (2024). *Official Journal of the European Union, L 1366*.

Cornelissen, J. (2017). Editor's comments: Developing propositions, a process model, or a typology? Addressing the challenges of writing theory without a boilerplate. *Academy of Management Review, 42*(1), 1–9. https://doi.org/10.5465/amr.2016.0196

Cuganesan, S., Steele, C., & Hart, A. (2018). How senior management and workplace norms influence information security attitudes and self-efficacy. *Behaviour & Information Technology, 37*(1), 50–65. https://doi.org/10.1080/0144929X.2017.1397193

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

da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002

da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security, 70*, 72–94. https://doi.org/10.1016/j.cose.2017.05.002

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security, 92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

Demirel, Y. (2012). Energy and energy types. In *Energy* (pp. 13–36). Springer. https://doi.org/10.1007/978-1-4471-2372-9_2

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

Deva, P. M., & Suchithra, M. C. (2020). The Personal Data Protection Bill, 2018: India's regulatory journey towards a comprehensive data protection law. *International Journal of Law and Information Technology, 28*(1), 1–19. https://doi.org/10.1093/ijlit/eaaa003

Dharmalingam, R., Shivasankarappa, A., & Neelamegam, A. (2018). A novel approach for optimizing governance, risk management and compliance for enterprise information security using DEMATEL and FoM. *Procedia Computer Science, 134,* 365–370. https://doi.org/10.1016/j.procs.2018.07.197

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of network and information systems across the Union (NIS Directive). (2016). *Official Journal of the European Union, L 194*, 1–30.

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security, 28*(3–4), 189–198. https://doi.org/10.1016/j.cose.2008.11.007

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). IEEE. https://doi.org/10.1109/CPRE.2011.6035634

Ebert, N., Schaltegger, T., Ambuehl, B., Schöni, L., Zimmermann, V., & Knieps, M. (2023). Learning from safety science: A way forward for studying cybersecurity incidents in organizations. *Computers & Security, 134*, 103435. https://doi.org/10.1016/j.cose.2023.103435

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 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 (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.

European Parliament & Council of the 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, 80–152.

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. *IEEE Access, 10*, 134038–134051. https://doi.org/10.1109/ACCESS.2022.3231847

Fiore, A. P. A., Facin, A. L. F., & Muniz Jr., J. (2023). Information security and quality management systems integration: Challenges and critical factors. *International Journal for Quality Research, 17*(3), 635–650. https://doi.org/10.24874/IJQR17.03-01

Gcaza, N., & von Solms, R. (2017). Cybersecurity culture: An ill-defined problem. In M. Bishop, L. Futcher, N. Miloslavskaya, & M. Theocharidou (Eds.), *Information security education for a global digital society* (Vol. 503, pp. 111–120). Springer. https://doi.org/10.1007/978-3-319-58553-6_9

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems, 62*(3), 452–462. https://doi.org/10.1080/08874417.2020.1845583

Gerber, M., & von Solms, R. (2008). Information security requirements – Interpreting the legal aspects. *Computers & Security, 27*(5–6), 124–135. https://doi.org/10.1016/j.cose.2008.07.009

Gericke, A., Fill, H.-G., Karagiannis, D., & Winter, R. (2009). Situational method engineering for governance, risk, and compliance information systems. In *Proceedings of the 2009 ACM Symposium on Applied Computing* (pp. 1281–1287). https://doi.org/10.1145/1555619.1555651

Golmohamadi, H., & Keypour, R. (2017). Retail energy management in electricity markets: Structure, challenges and economic aspects – a review. *Technology and Economics of Smart Grids and Sustainable Energy, 2*(1), 20. https://doi.org/10.1007/s40866-017-0036-3

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*, Article 15. https://doi.org/10.1186/s42162-018-0019-1

Gravina, N., Nastasi, J., & Austin, J. (2021). Assessment of employee performance. *Journal of Organizational Behavior Management, 41*(2), 124–149. https://doi.org/10.1080/01608061.2020.1869136

Grigaliūnas, Š., Schmidt, M., Brūzgienė, R., Smyrli, P., Andreou, S., & Lopata, A. (2024). Holistic information security management and compliance framework. *Electronics, 13*(19), 3955. https://doi.org/10.3390/electronics13193955

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of AI-driven cyber attacks: A review. *Applied Artificial Intelligence, 36*(1). https://doi.org/10.1080/08839514.2022.2037254

Haber, E., & Zarsky, T. (2018). Cybersecurity for infrastructure: A critical analysis. *Florida State University Law Review, 44*(2). https://ir.law.fsu.edu/lr/vol44/iss2/3

Hadush, S. Y., & Meeus, L. (2018). DSO–TSO cooperation issues and solutions for distribution grid congestion management. *Energy Policy, 120*, 610–621. https://doi.org/10.1016/j.enpol.2018.05.065

Halliday, N. (2024). Advancing organizational resilience through enterprise GRC integration frameworks. *International Journal of Advanced Multidisciplinary Research and Studies, 4*(5). https://doi.org/10.62225/2583049X.2024.4.5.4888

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, 23*(15), 6716. https://doi.org/10.3390/s23156716

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

Herbane, B., Elliott, D., & Swartz, E. M. (2004). Business continuity management: Time for a strategic role? *Long Range Planning, 37*(5), 435–457. https://doi.org/10.1016/j.lrp.2004.07.011

Higashizawa, N., & Aihara, Y. (2017). Data privacy protection of personal information versus usage of big data: Introduction of the recent amendment to the Act on the Protection of Personal Information (Japan). *Defense Counsel Journal, 84*(4), 1–15.

Howard, M. C. (2016). A review of exploratory factor analysis decisions and overview of current practices: What we are doing and how can we improve? *International Journal of Human–Computer Interaction, 32*(1), 51–62. https://doi.org/10.1080/10447318.2015.1087664

Hseiki, H., El Hajj, A., Ajra, Y., Hija, F., & Haidar, A. (2024). A secure and resilient smart energy meter. *IEEE Access.* https://doi.org/10.1109/ACCESS.2023.3349091

Ilina, E., & Sundquist, H. (2012). An examination of nuclear power plants event reporting in the context of knowledge management. International Journal of Nuclear Knowledge Management, 5(4), 361–373. https://doi.org/10.1504/IJNKM.2011.045713

International Organization for Standardization. (2013). ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements.

International Organization for Standardization. (2019). ISO/IEC 27002:2019 — Information technology — Security techniques — Code of practice for information security controls.

International Organization for Standardization. (2022a). ISO/IEC 27001:2022 — Information technology — Security techniques — Information security management systems — Requirements.

International Organization for Standardization. (2022b). ISO/IEC 27002:2022 — Information technology — Security techniques — Information security controls.

Ioannou, M., Stavrou, E., & Bada, M. (2019). Cybersecurity culture in computer security incident response teams: Investigating difficulties in communication and coordination. *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 1–4. https://doi.org/10.1109/CyberSecPODS.2019.8885240

Jasiūnas, J., Lund, P. D., & Mikkola, J. (2021). Energy system resilience – A review. *Renewable and Sustainable Energy Reviews, 150*, 111476. https://doi.org/10.1016/j.rser.2021.111476

Javadnejad, F., Abdelmagid, A. M., Pinto, C. A., McShane, M., & Diaz, R. (2024). An exploratory data analysis of malware/ransomware cyberattacks: Insights from an extensive cyber loss dataset. *Enterprise Information Systems, 18*(9), Article 2369952. https://doi.org/10.1080/17517575.2024.2369952

Jiang, Y., Jeusfeld, M. A., Ding, J., & Sandahl, E. (2023). Model-based cybersecurity analysis. *Business & Information Systems Engineering, 65*(6), 643–676. https://doi.org/10.1007/s12599-023-00811-0

Jurgens, J., & Dal Cin, P. (2025, January 13). *Global cybersecurity outlook 2025*. World Economic Forum. https://www.weforum.org/reports/global-cybersecurity-outlook-2025

Järveläinen, J. (2013). IT incidents and business impacts: Validating a framework for continuity management in information systems. *International Journal of Information Management, 33*(4), 583–590. https://doi.org/10.1016/j.ijinfomgt.2013.03.001

Järveläinen, J., Dang, D., Mekkanen, M., & Vartiainen, T. (2025). Towards a framework for improving cyber security resilience of critical infrastructure against cyber threats: A dynamic capabilities approach. *Journal of Decision Systems, 34*(1). https://doi.org/10.1080/12460125.2025.2479546

Khajouei, H., Kazemi, M., & Moosavirad, S. H. (2017). Ranking information security controls by using fuzzy analytic hierarchy process. *Information Systems and eBusiness Management, 15*(1), 1–19. https://doi.org/10.1007/s10257-016-0306-y

Klich, A. (2023). Personal data protection in the energy services market – selected issues. *Journal of Modern Science, 51*, 645–668. https://doi.org/10.13166/jms/168314

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. *arXiv*. https://doi.org/10.48550/arXiv.2403.08036

Lee, A. S., & Baskerville, R. L. (2003). Generalizing generalizability in information systems research. *Information Systems Research, 14*(3), 221–243. https://doi.org/10.1287/isre.14.3.221.16560

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

Leidner, D. E. (2020). What's in a contribution. *Journal of the Association for Information Systems, 21*(1), 238–245. https://doi.org/10.17705/1jais.00598

Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry, 103*, 97–110. https://doi.org/10.1016/j.compind.2018.09.004

Li, Y., Koppenjan, J., & Wang, H. (2024). Individual, organizational, and institutional accountability: A systematic literature review in public administration. *Public Management Review*. https://doi.org/10.1080/14719037.2024.2369799

Lopes, M. I., Guarda, T., & Oliveira, P. (2019). Implementation of ISO 27001 standards as GDPR compliance facilitator. *Journal of Information Systems Engineering and Management, 4*(2).

Lundgren, B., & Möller, N. (2019). Defining information security. *Science and Engineering Ethics, 25*(2), 419–441. https://doi.org/10.1007/s11948-017-9992-1

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

Macedo, A. C. (2021). Some thoughts about the intersection between data protection and competition law: A view from Brazil. *Journal of Antitrust Enforcement, 9*(2), 197–202. https://doi.org/10.1093/jaenfo/jnab007

Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. (2017). A systematic literature review: Information security culture. In *Proceedings of the 2017 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICRIIS.2017.8002442

Mallick, M. A. I., & Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. World Scientific News, 190(1), 1–69.

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

Mayer, N., & De Smet, D. (2017). Systematic literature review and ISO standards analysis to integrate IT governance and security risk management. *International Journal for Infonomics, 10*(1). https://doi.org/10.20533/IJI.1742.4712.2017.0154

Meagher, H., & Dhirani, L. L. (2024). Cyber-resilience, principles, and practices. In K. N. Qureshi, T. Newe, G. Jeon, & A. Chehri (Eds.), *Cybersecurity vigilance and security engineering of Internet of Everything (Internet of Things)*. Springer. https://doi.org/10.1007/978-3-031-45162-1_4

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

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

Müller, N., Afzal, Z., Eliasson, P., Ekstedt, M., & Heussen, K. (2023). Threat scenarios and monitoring requirements for cyber-physical systems of flexibility markets. *arXiv*. https://doi.org/10.48550/arXiv.2111.03300

Muqeet, H. A., Ahmad, A., Sajjad, I. A., Liaqat, R., Raza, A., & Iqbal, M. M. (2019). Benefits of distributed energy and storage system in prosumer based electricity market. In *2019 IEEE International Conference on Environment and Electrical Engineering and 2019 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe)* (pp. 1–6). IEEE. https://doi.org/10.1109/EEEIC.2019.8783636

Murray, G., Johnstone, M. N., & Valli, C. (2017). The convergence of IT and OT in critical infrastructure. In C. Valli (Ed.), The proceedings of the 15th Australian Information Security Management Conference, 5–6 December 2017, Edith Cowan University, Perth, Western Australia (pp. 149–155). Edith Cowan University. https://ro.ecu.edu.au/ism/217

Nasir, A., Arshah, R. A., Ab Hamid, M. R., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications, 44*, 12–22. https://doi.org/10.1016/j.jisa.2018.11.003

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

Nicho, M., Khan, S., & Rahman, M. S. M. K. (2017). Managing information security risk using integrated governance, risk, and compliance. In *2017 International Conference on Computer and Applications (ICCA)* (pp. 56–66). IEEE. https://doi.org/10.1109/COMAPP.2017.8079741

Niemimaa, M., Järveläinen, J., Heikkilä, M., & Heikkilä, J. (2019). Business continuity of business models: Evaluating the resilience of business models for contingencies. *International Journal of Information Management, 49*, 208–216. https://doi.org/10.1016/j.ijinfomgt.2019.04.010

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

Papazafeiropoulou, A., & Spanaki, K. (2015). Understanding governance, risk, and compliance information systems (GRC IS): The experts' view. *Information Systems Frontiers, 18*(1), 1–18. https://doi.org/10.1007/s10796-015-9572-3

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

Pearson, H., & Sutherland, M. (2017). The complexity of the antecedents influencing accountability in organisations. *European Business Review, 29*(4), 419–439. https://doi.org/10.1108/EBR-08-2016-0106

Peerally, M. F., Carr, S., Waring, J., & Dixon-Woods, M. (2017). The problem with root cause analysis. *BMJ Quality & Safety, 26*(5), 417–422. https://doi.org/10.1136/bmjqs-2016-005511

Presthus, W., & Sønslien, K. F. (2021). An analysis of violations and sanctions following the GDPR. *International Journal of Information Systems and Project Management, 9*(1), 38–53. https://doi.org/10.12821/ijispm090102

Ramachandran, S., Rao, V. S. C., Goles, T., & Dhillon, G. (2013). Variations in information security cultures across professions: A qualitative study. *Communications of the Association for Information Systems, 33*(11), 163–204. https://doi.org/10.17705/1CAIS.03311

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union (OJ L 1689, 12.7.2024).

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). Official Journal of the European Union.

Ridha, E., Nolting, L., & Praktiknjo, A. (2020). Complexity profiles: A large-scale review of energy system models in terms of complexity. *Energy Strategy Reviews, 30*, 100515. https://doi.org/10.1016/j.esr.2020.100515

Rodrigues, R. B., & Filho, G. K. O. (2025). Fostering a culture of transparency: Leadership's role in enhancing self-reporting practices in aviation safety. Next Research, 2(2), 100290. https://doi.org/10.1016/j.nexres.2025.100290

Rooney, J. J., Lee, N., & Vanden Heuvel, L. N. (2004). Root cause analysis for beginners. *Quality Progress, 37*(7), 45–53.

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). Developing cyber-resilient systems: A systems security engineering approach (NIST Special

Publication No. 800-160 Vol. 2 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1

Ruohonen, J., & Hjerppe, K. (2022). The GDPR enforcement fines at a glance. *Information Systems, 106,* 101876. https://doi.org/10.1016/j.is.2021.101876

Saeed, S., Gull, H., Aldossary, M. M., Altamimi, A. F., Alshahrani, M. S., Saqib, M., Zafar Iqbal, S., & Almuhaideb, A. M. (2024). Digital transformation in energy sector: Cybersecurity challenges and implications. *Information, 15*(12), 764. https://doi.org/10.3390/info15120764

Salama, R., Altrjman, C., & Al-Turjman, F. (2024). Healthcare cybersecurity challenges: A look at current and future trends. In F. Al-Turjman (Ed.), *Computational intelligence and blockchain in complex systems* (pp. 97–111). Morgan Kaufmann. https://doi.org/10.1016/B978-0-443-13268-1.00003-0

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2023). *Research methods for business students* (9th ed.). Pearson Education.

Schlaile, M. P., Bogner, K., & Muelder, L. (2021). It's more than complicated! Using organizational memetics to capture the complexity of organizational culture. *Journal of Business Research, 129*, 801–812. https://doi.org/10.1016/j.jbusres.2019.09.035

Schwartz, M. S. (2001). The nature of the relationship between corporate codes of ethics and behaviour. *Journal of Business Ethics, 32*, 247–262. https://doi.org/10.1023/A:1010787607771

Shah, R. (2023). *Getting regulation right: Approaches to improving Australia's cybersecurity* (Policy Brief Report No. 73/2023). Australian Strategic Policy Institute (ASPI).

Sherif, E., Furnell, S., & Clarke, N. (2015). An identification of variables influencing the establishment of information security culture. In T. Tryfonas & I. Askoxylakis (Eds.), *Human aspects of information security, privacy, and trust* (Lecture Notes in Computer Science, Vol. 9190, pp. 436–448). Springer. https://doi.org/10.1007/978-3-319-20376-8_39

Shoetan, P. O., Amoo, O. O., Okafor, E. S., & Olorunfemi, O. L. (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

Shojaie, B., Federrath, H., & Saberi, I. (2014). Evaluating the effectiveness of ISO 27001:2013 based on Annex A. In *2014 Ninth International Conference on Availability, Reliability and Security (ARES)* (pp. [insert page numbers]). IEEE. https://doi.org/10.1109/ARES.2014.41

Shrestha, N. (2021). Factor analysis as a tool for survey analysis. *American Journal of Applied Mathematics and Statistics, 9*(1), 4–11. https://doi.org/10.12691/ajams-9-1-2

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267–270. https://doi.org/10.1016/j.im.2008.12.007

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. In *Proceedings of the Eleventh Workshop on Visualization for Cyber Security (VizSec '14)* (pp. 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.

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. JOIV: International Journal on Informatics Visualization, 4(4), 225–230.

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

Sun, C.-C., Cardenas, D. J. S., Hahn, A., & Liu, C.-C. (2020). Intrusion detection for cybersecurity of smart meters. *IEEE Transactions on Smart Grid, 12*(1), 612–622. https://doi.org/10.1109/TSG.2020.3010230

Sutton, A., & Tompson, L. (2025). *Towards a cybersecurity culture-behaviour framework: A rapid evidence review. Computers & Security, 148*, 104110. https://doi.org/10.1016/j.cose.2024.104110

Syafrizal, M., Selamat, S. R., & Zakaria, N. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security, 12*(3), 417–432. https://doi.org/10.17762/ijcnis.v12i3.4817

Symantec. (2024). *Cybersecurity for retail services: Strategies that empower your business, drive innovation, and build customer trust*. Broadcom. https://docs.broadcom.com/doc/cybersecurity-retail-en

Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: A case study. *Information Technology & Management, 17*, 179–186. https://doi.org/10.1007/s10799-015-0252-2

Tariq, M. T., Tayyaba, S., Ali, M. T., Safraz, M. S., De-La-Hoz-Franco, E., Butt, S. A., Starcangelo, V., & Rad, D. V. (2020). Combination of AHP and TOPSIS methods for the ranking of information security controls to overcome its obstructions under fuzzy environment. *Journal of Intelligent & Fuzzy Systems, 38*(5), 6075–6088. https://doi.org/10.3233/JIFS-179692

Thomas, I. (2020). Getting ready for the California Consumer Privacy Act: Building on General Data Protection Regulation preparedness. *Applied Marketing Analytics: The Peer-Reviewed Journal, 5.* https://doi.org/10.69554/OLHS2696

Tolah, A., Furnell, S. M., & Papadaki, M. (2021). An empirical analysis of the information security culture key factors framework. *Computers & Security, 108*, 102354. https://doi.org/10.1016/j.cose.2021.102354

Truță, F. (2020, April 15). Portuguese energy company hit with Ragnar Locker ransomware; Attackers demand $10 million to decrypt the data. *Bitdefender*. https://www.bitdefender.com/en-us/blog/hotforsecurity/portuguese-energy-company-hit-with-ragnar-locker-ransomware-attackers-demand-10-million-to-decrypt-the-data

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

Uchendu, B., Nurse, J. R. C., & Furnell, S. (2021). Developing a cybersecurity culture: Current practices and future needs. *Computers & Security, 109*, 102387. https://doi.org/10.1016/j.cose.2021.10238

UK Government. (2025, August 20). List of acceptable proof of address documents for countersignatories. *GOV.UK*. https://www.gov.uk/government/publications/horizon-shortfall-scheme-appeals-proving-your-identity/list-of-acceptable-proof-of-address-documents-for-countersignatories

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., & Bellekens, X. (2022). Cyber-security challenges in aviation industry: A review of current and future trends. *Information, 13*(3), 146. https://doi.org/10.3390/info13030146

Vaibhav, A. (2022). Information security governance metrics: A survey and taxonomy. *Information Security Journal: A Global Perspective, 31*(4), 466–478. https://doi.org/10.1080/19393555.2021.1922786

Vaka, P. R. (2025). Cybersecurity in the retail industry. *International Research Journal of Modernization in Engineering Technology and Science, 7*(2), 939–947.

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

Vicente, P., & da Silva, M. M. (2011). A business viewpoint for integrated IT governance, risk, and compliance. In *2011 IEEE World Congress on Services* (pp. 422–428). IEEE. https://doi.org/10.1109/SERVICES.2011.62

Vincent, N. E., Higgs, J. L., & Pinsker, R. E. (2019). Board and management-level factors affecting the maturity of IT risk management practices. *Journal of Information Systems, 33*(3), 117–135. https://doi.org/10.2308/isys-52229

von Solms, B. (2000). Information security – The third wave? *Computers & Security, 19*(7), 615–620. https://doi.org/10.1016/S0167-4048(00)07021-8

von Solms, B. (2001). Information security—A multidimensional discipline. *Computers & Security, 20*(6), 504–508. https://doi.org/10.1016/S0167-4048(01)00608-3

von Solms, B. (2006). Information security – The fourth wave. *Computers & Security, 25*(3), 165–168. https://doi.org/10.1016/j.cose.2006.03.004

von Solms, S. H. (2010). The 5 waves of information security – From Kristian Beckman to the present. In K. Rannenberg, V. Varadharajan, & C. Weber (Eds.), *Security and privacy – Silver linings in the cloud. SEC 2010* (IFIP Advances in Information and Communication Technology, Vol. 330, pp. 3–17). Springer. https://doi.org/10.1007/978-3-642-15257-3_1

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

Vuong, T. D. N., & Nguyen, L. T. (2022). The key strategies for measuring employee performance in companies: A systematic review. *Sustainability, 14*(21), 14017. https://doi.org/10.3390/su142114017

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

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

Wolff, J., & Atallah, N. (2021). Early GDPR penalties: Analysis of implementation and fines through May 2020. *Journal of Information Policy, 11,* 63–103. https://doi.org/10.5325/jinfopoli.11.2021.0063

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. (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

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

Publications

[1] Suorsa, M., Helo, P., & Petman, J. (2025). *Key drivers of information security culture: A survey and exploratory factor analysis in an energy retail organization* [Manuscript submitted for publication]. *Information Security Journal: A Global Perspective*. © 2025 The Author(s). This manuscript is included in the dissertation with the permission of the co-authors.

[2] Suorsa, M., & Helo, P. (2023). *Information security failures identified and measured: ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis* [Peer-reviewed journal article]. *Information Security Journal: A Global Perspective, 33*(3), 285–306. https://doi.org/10.1080/19393555.2023.2270984. © 2023 Taylor & Francis Group, LLC. Reproduced with permission in accordance with the publisher's dissertation reuse policy.

[3] Suorsa, M., & Helo, P. (2023). *Information security failures measured and ISO/IEC 27001:2022 controls ranked by General Data Protection Regulation penalty analysis* [Conference paper]. In *Proceedings of the 2023 11th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1–5). Makassar, Indonesia. https://doi.org/10.1109/CITSM60085.2023.10455413. © 2023 IEEE. Reprinted with permission in accordance with IEEE thesis reuse guidelines.

[4] Suorsa, M., & Helo, P. (2025). *Cybersecurity risks and defense for a European energy retail business: A case study using FMEA and Bowtie incident analysis* [Peer-reviewed journal article]. *Information Security Journal: A Global Perspective*, 1–29. https://doi.org/10.1080/19393555.2025.2489421. © 2025 Taylor & Francis Group, LLC. Reproduced with permission in accordance with the publisher's dissertation reuse policy.

Key Drivers of Information Security Culture: A Survey and Exploratory Factor Analysis in an Energy Retail Organization

Suorsa, M.,[a]* Helo, P., [b] and Petman, J.[c]

[a]*School of Technology and Innovations, University of Vaasa, Vaasa, Finland, k83110@student.uwasa.fi, ORCiD: 0000-0002-1649-4223*

[b]*School of Technology and Innovations, University of Vaasa, Vaasa, Finland petri.helo@uwasa.fi, ORCiD: 0000-0002-0501-2727*

[c]*Department of Mathematics and Statistics, University of Jyväskylä, Jyväskylä, Finland joni.petman@gmail.com, ORCiD: 0009-0002-6394-9777*

Mikko Suorsa is a Ph.D. student in Industrial Management at the University of Vaasa, Finland. He holds master's degrees in both Industrial Management and Public Administration and is positioned in a large international energy corporation as the Business Information Security Officer. His research interests include information security governance, standardization, data protection, and regulatory compliance.

Petri Helo is Professor of Industrial Management, Logistics Systems, and head of the Networked Value Systems research group at the School of Technology and Innovations, University of Vaasa, Finland. His research addresses the management of supply chains and use of information technology in operations.

Joni Petman holds a Master of Philosophy degree in Statistics from the University of Jyväskylä, Finland. He works as a Data Analyst at a large international energy corporation. His research interests include business analytics and statistical methods.

Key Drivers of Information Security Culture: A Survey and Exploratory Factor Analysis in an Energy Retail Organization

Abstract

The energy retail sector is foundational to the energy industry value chain, making the strengthening of its information security culture an organizational necessity. This study examines the factors that influence information security culture in European energy retail businesses, based on a survey developed from insights gained through a narrative literature review and conducted within an energy retail organization. A total of 610 employees completed the survey, resulting in a 29% response rate, and an Exploratory Factor Analysis (EFA) was subsequently performed to identify the underlying key drivers of information security culture. These include: (1) Management engagement in information security, (2) Inclusion of information security in formal performance appraisal and (3) Assignment of responsibility for information security reporting. Theoretically, this study contributes to the field of IT Governance, Risk Management, and Compliance (IT-GRC) within the critical energy sector, while its findings provide a practical executive summary for strengthening information security culture strategies within energy retail organizations.

Keywords: Energy Retail Sector; Exploratory Factor Analysis; Information Security Culture; Survey

1. Introduction

Energy powers critical infrastructure, making information security necessary for societal resilience, as nearly all essential processes depend on a stable energy supply (Yusta et al., 2011; Löschel et al., 2010). As the energy retail sector supplies energy and provides solutions to businesses and consumers, it is fundamental to maintaining essential services (European Union, 2022) and is a prime target for cybercriminals due to its financial value (Dagoumas, 2019).

The increasing frequency and sophistication of cyberattacks pose national security risks and disrupt operations (Falowo et al., 2022). These incidents can lead to severe

financial losses, data breaches, legal liabilities, and reputational damage (Lis & Mendel, 2019). Recent examples of cyberattacks on critical energy infrastructure include the Ukraine power grid attack, which caused major blackouts (Sullivan & Kamensky, 2017); the ransomware incident targeting the U.S. Colonial Pipeline, which led to fuel shortages and economic disruption (Beerman et al., 2023); and the cyberattack on Saudi Aramco, which resulted in extensive financial losses (Bronk & Tikk-Ringas, 2013).

Strengthening the resilience of energy infrastructure has become both urgent and paramount due to the increasing frequency of cyberattacks amid geopolitical tensions (Aljohani, 2024), and it is recognized as a global megatrend driven by regulatory developments (Haber & Zarsky, 2018). In the European Union (EU), a recent example of regulatory development is the Network and Information Security Directive 2 (NIS 2 Directive), which mandates a risk-based approach to cybersecurity resilience and enforces substantial monetary penalties for noncompliance (European Union, 2022).

Similar regulatory developments globally include the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) in the United States, which mandates the timely reporting of significant cyber incidents and ransomware payments by critical infrastructure entities (Folio III et al., 2025). Other notable examples include Australia's Security of Critical Infrastructure Act (Lloyd-Jones, 2025), Singapore's Cybersecurity Act (Gorian, 2025), and Japan's Cybersecurity Management Guidelines for Critical Infrastructure (Mochinaga, 2024).

Cybersecurity culture within the energy sector shapes organisational practices and employee behaviour aimed at protecting critical assets, data, and information, thereby enhancing resilience and establishing security as a strategic priority (AlHogail & Mirza, 2014a). The strengthening of information security culture is positioned within the organization's IT governance, risk management, and compliance (IT-GRC) function

(Adeyinka et al., 2024). While the factors driving the strengthening of information security culture have been extensively explored (Alnatheer, 2015; Sherif et al., 2015; Uchendu et al., 2021), their specific underlying impacts and contributing mechanisms remain unclear (Gcaza & von Solms, 2017; AlHogail & Mirza, 2014a).

Management engagement is the most frequently cited factor influencing cybersecurity culture; however, it alone is insufficient, and the impact of other contributing factors warrants further exploration (Uchendu et al., 2021). These observations underscore the need for continued investigation into the drivers of cybersecurity culture (Gcaza & von Solms, 2017), particularly within the energy retail sector, where existing research remains limited.

This study uses the concepts "information security" and "cybersecurity" interchangeably. While cybersecurity focuses on protecting digital information (von Solms & van Niekerk, 2013), information security has a broader scope, encompassing physical assets and organizational practices, and is integrated into corporate governance structures (von Solms, 2000).

The importance of cybersecurity culture continues to grow, driven by the increasing number and sophistication of cyberattacks, rising regulatory demands, and the need to bridge gaps in existing research. This study examines the factors that strengthen information security culture within the energy retail sector. The primary research question guiding this study is:

- What are the key factors that drive the strengthening of information security culture in energy retail organizations?

Data were collected through a survey conducted within a large European energy retail organization, yielding 610 completed responses and representing a 29% employee

response rate. The survey was developed based on insights from a narrative literature review, ensuring that the questions addressed the key dimensions of information security culture identified in prior research.

To analyze the survey data, this study employs exploratory factor analysis (EFA), a statistical method that identifies underlying relationships among survey variables by grouping related items into key factors. This approach reduces data complexity and reveals structural patterns (Shrestha, 2021), providing actionable recommendations to support the strengthening of information security culture in energy retail businesses.

The remainder of the paper is structured as follows. Section 2 outlines the study's methodology, while Section 3 presents the results. Section 4 provides a discussion of the findings, and Section 5 concludes by summarizing the study's contributions, acknowledging its limitations, and offering directions for future research.

2. Methodology

This section outlines the methodology employed in the study, including the approach and findings of the narrative literature review, as well as the design and administration of the survey. Subsequently, exploratory factor analysis (EFA) is applied to interpret and analyze the survey data.

2.1 Narrative literature review approach

A narrative literature review was conducted following the approach proposed by Ferrari (2015), providing an interpretive and integrative synthesis of existing knowledge rather than an exhaustive catalogue of studies. Its purpose was twofold: to identify key factors influencing information security culture in European energy retail organizations, and to inform the development of survey questions capturing organizational and behavioral aspects of cybersecurity.

The review drew exclusively on peer-reviewed journal articles. Major databases searched included Scopus, Web of Science, IEEE Xplore, and Google Scholar, using keywords such as “information security culture,” “organizational culture information security,” “IT governance, risk management, and compliance (IT-GRC),” “security awareness,” “cybersecurity behavior,” “management commitment to information security,” “risk perception information security,” “security reporting culture,” “security compliance behavior,” “human factors cybersecurity,” and “ISO/IEC 27001 adoption,” with Boolean operators applied to ensure precise coverage.

Publications in English from 2003 to 2025 were included, with influential earlier works also considered where relevant (e.g., Schein, 1996; von Solms, 2006). Studies focusing exclusively on technical controls or non-organizational contexts were excluded.

This review highlighted key organizational, managerial, and behavioral factors that shape information security culture, including governance, risk management, policy compliance, management commitment, employee awareness, reporting, trust, teamwork, and performance assessment. These factors are reflected in Table 1 and directly informed the design of the survey used in the empirical phase of the study.

To guide both survey design and analysis, the study adopted the Cyber Security Culture Framework proposed by Georgiadou et al. (2022), which conceptualizes cybersecurity as an ecosystem operating at both organizational and individual levels. At the organizational level, the framework identifies:

- Assets: people, systems, facilities, and information, protected through appropriate policies
- Access and trust: role-based permissions to information and interactions with third parties
- Operations: efficient business processes integrating security considerations

- Defense: proactive technical planning and system configurations
- Security governance: planning, managing, and continuously improving security practices

At the individual level, it highlights:

- Awareness: knowledge of security issues
- Behavior: daily security-conscious actions
- Competency: skills and expertise to comply with security policies

These dimensions illustrate the interplay among structural, technical, and human factors in cybersecurity and support informing the survey questions in Table 1, which cover both organizational and individual aspects.

2.2 Narrative literature review findings on information security culture

Strengthening information security culture is positioned within an organization's IT Governance, Risk Management, and Compliance (IT-GRC) function (Nicho et al., 2017). Within the three interrelated domains of IT-GRC, governance defines the organization's strategy, key objectives, culture, risk appetite, and policies (Vicente & da Silva, 2011). Risk management seeks to balance these strategic goals with the need to protect against potential losses, while compliance ensures adherence to external laws and standards, as well as internal organizational policies (Adeyinka et al., 2024).

IT-GRC both shapes and is shaped by an organization's cultural, social, and political environment. Its effectiveness relies on alignment with the organization's values, norms, and behaviors (Papazafeiropoulou & Spanaki, 2015), offering several organizational benefits (Ali et al., 2021). When employees understand compliance principles, they are more likely to ask questions, make ethical decisions, and report

violations. Over time, a positive and transparent compliance culture reinforces shared values and strengthens commitment to organizational objectives (Schwartz, 2001).

Despite its benefits, a common challenge in implementing IT-GRC is the tendency to overlook organizational culture (Adeyinka et al., 2024), as cultural factors are often complex, difficult to conceptualize, and challenging to measure (Schlaile et al., 2021). However, if unmanaged, culture can influence organizations and their employees without their conscious knowledge (Schein, 1996).

Furthermore, while information security culture shapes how employees act, technological measures alone cannot fully protect the organization. Therefore, greater emphasis should be directed towards users' behavioral aspects (Tang et al., 2016; Mahfuth et al., 2017), as even the most comprehensively protected organization remains vulnerable without an effective security culture (Georgiadou et al., 2022). Therefore, further research is needed on IT-GRC success factors, particularly those related to cultural elements (Gericke et al., 2009).

International standardization frameworks play a significant role in managing information security risk within the organizational IT-GRC structure (Siponen & Willison, 2009; Sanskriti & Astitwa, 2018). A wide variety of information security standards are available, such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) (National Institute of Standards and Technology, 2024) and Control Objectives for Information and Related Technologies (COBIT) (Information Systems Audit and Control Association [ISACA], 2018). Notably, ISO/IEC 27001 is the most widely adopted standard and is considered the de facto approach to managing information security (Sulistyowati et al., 2020; ISO/IEC 27001:2022).

Organizations with ISO/IEC 27001 certification exhibit heightened awareness of cybersecurity risks (Putri et al., 2024) and strengthen incident response practices,

regulatory compliance, and a consistent security-first mindset across departments (Folorunso et al., 2024). Beyond technical measures, ISO/IEC 27001 also shapes human factors, enhancing employees' security behavior and knowledge-sharing while reinforcing a security-conscious culture throughout the organization (Kör & Metin, 2021).

An organization's information security culture is characterized by the shared attitudes, beliefs, and knowledge that drive behavior and decision-making. It shapes strategic direction and guides operations to protect the confidentiality, integrity, and availability of organizational assets, thereby serving as a substantial contributor to risk management and organizational resilience (da Veiga & Eloff, 2010; Von Solms, 2006).

Employees' perception of information security risks constitutes a critical domain within organizational culture (da Veiga & Martins, 2017). It involves understanding which assets require protection, and why, enabling timely security responses aligned with the organization's risk landscape and resilience objectives (Nasir et al., 2019). A lack of awareness among employees regarding information security risks can result in significant losses, particularly when such risks are overlooked or underestimated (Tang et al., 2016). A risk-aware employee recognizes their exposure to information security threats in daily work, which informed the formulation of Question ID 1 in the survey. Table 1 presents the complete set of survey questions.

Employee awareness represents a fundamental domain influencing cybersecurity culture (Wiley et al., 2020) and has been extensively investigated in the academic literature (cf. Khando et al., 2021; Tolah et al., 2021). Non-compliant behaviors are often unintentional and caused by human error arising from lack of awareness, rather than deliberate misconduct or malicious intent (Parsons et al., 2014).

ID	Question	Culture domain	Culture at the individual level	Culture at the organizational level
1	I am often exposed to information security threats at work	Information security risk perception	Awareness	Defense
2	I am familiar with the company's written rules, responsibilities, and expected behaviors regarding information security	Information security policy awareness	Awareness	Security governance
3	I find these rules, responsibilities, and expectations clear	Information security policy compliance	Competency	Security governance
4	It is easy and frictionless for me to comply with these expectations	Information security policy compliance	Attitude	Operations
5	My direct managers or supervisors have clearly explained the importance of security to me	Management engagement in information security	Awareness	Security governance
6	The management team of the company has conveyed the importance of security	Management engagement in information security	Awareness	Security governance
7	Security is a part of my daily work routines	Information security responsibility	Behaviour	Operations
8	I feel personally responsible for maintaining the security of the company's digital assets and information	Information security responsibility	Attitude	Assets
9	I would report a cybersecurity issue if I noticed it. For example, a co-worker who continuously neglects security practices	Assignment of responsibility for information security reporting	Behaviour	Access and trust
10	If I accidentally caused a cybersecurity incident, I would immediately report it. For example, if I accidentally sent company information to the wrong recipient	Assignment of responsibility for information security reporting	Behaviour	Access and trust
11	I am confident in my ability to handle information in a secure way	Information security self-efficacy	Competency	Defence
12	In my team we correct and help each other to be more secure	Information security teamwork	Behaviour	Access and trust
13	Delivering on security responsibilities is considered in my overall performance assessment	Inclusion of information security in formal performance appraisal	Awareness	Security governance
14	I am aware of what information assets I am responsible for and how to protect these	Information security policy awareness	Competency	Assets
15	In my team, good security behavior (i.e. doing the right thing) is rewarded	Inclusion of information security in formal performance appraisal	Awareness	Security governance
16	I understand how to classify/label information within the company's guidelines	Information security policy compliance	Competency	Assets
17	An employee from the IT department asks you to click a link to perform a system update. How likely are you to click the link in this situation?	Information security policy behavior	Behaviour	Defence
18	An employee shares their password with a co-worker. How likely are you to do the same in this situation?	Information security policy behavior	Behaviour	Access and trust

Table 1. Survey questions

Consequently, fostering information security awareness requires clear and consistent communication, alongside ongoing training initiatives aimed at cultivating employee commitment to expected security practices (Adeyinka et al., 2024). Furthermore, employees' responsibility for asset ownership should be both encouraged and formalized, as this promotes informed decision-making and proactive security behaviors necessary for protecting these assets (Fenz et al., 2014). These principles informed the development of Questions ID 2 and 14 in the survey.

The knowledge required by employees to adhere to information security policies often extends beyond their core job functions (van Niekerk & von Solms, 2010). Therefore, the quality of the information provided, including its relevance, accuracy, and clarity, is a significant determinant of how effectively employees can adhere to these policies, instructions, and expectations (Pahnila et al., 2007).

Moreover, regarding compliance with information security policies, actual end-user behavior is the core objective (Ali et al., 2021). Although the Theory of Planned Behavior has been extensively applied to this area (Sommestad et al., 2019), understanding exactly how its factors drive the shift from noncompliance to compliance remains challenging (Ali et al., 2009). Aspects of information security policy compliance are explored through Questions ID 3, 4, and 16, while user behavior is investigated using Questions ID 17 and 18 of the survey.

A well-researched and widely endorsed dimension in shaping information security culture is the active commitment and communication of top management (Vincent et al., 2018; Hu et al., 2012). This commitment is demonstrated through financial investments in security initiatives, visible advocacy for cybersecurity, and executive oversight of organizational practices (Reegård et al., 2019). Managerial engagement raises employee awareness and encourages adherence to expected security practices (Wiley et al., 2020).

Leadership commitment shapes employees' attitudes directly and influences behavior indirectly through organizational norms and values at both the individual and team level, promoting a collective sense of responsibility and prioritization of secure practices throughout the organization (Sharma & Aparicio, 2022). This dimension of management commitment is reflected in Questions ID 5 and 6 in the survey (Cuganesan et al., 2018).

An impactful information security culture is founded on accountability, with employees internalizing security tasks as personal responsibility (AlHogail, 2015). At the same time, top management holds ultimate accountability and steers strategic decisions to establish a responsible organization (Veiga & Eloff, 2002).

When staff feel accountable for safeguarding information, it strengthens the organization's collective sense of responsibility (AlHogail, 2015), making expected behavior a natural practice (Veiga & Eloff, 2002), which is closely linked to strengthening information security through the ethical conduct of an organization (Alnatheer, 2015). These responsibility-based principles guide the formulation of survey questions ID 7 and 8.

Moreover, a successful cybersecurity culture relies on learning from incidents to uncover and address their root causes to prevent similar incidents recurring (Patterson et al., 2023). In contrast, cyber risks are potential threats that could exploit vulnerabilities within organizational assets and result in incidents materializing (Strupczewski, 2021).

The prioritized reporting and treatment of cybersecurity risks and incidents indicate a mature security culture (Valavanis, 2024). This underscores the importance of initiatives that enhance employees' sense of responsibility in recognizing and reporting risks and incidents, a key step toward improving the overall culture of reporting behavior (Ahola et al., 2024). The formulation of survey questions ID 9 and 10 is guided by these reporting-based principles.

The concept of overarching organizational trust is central to the cultivating of an efficient cybersecurity culture. Mutual trust enhances collaboration and aligns knowledge, needs, and behaviors between employers and employees (da Veiga et al., 2020). Trust encompasses not only users' confidence in their ability to safeguard information, but also their belief that the organization communicates expectations and

information consistently and reliably (Veiga & Martins, 2014). This element informs survey Question ID 11.

Information security culture shapes group dynamics and team performance (Yoo et al., 2020), while trust, cooperation, information sharing, and communication define teams' everyday operations (Ioannou et al., 2019). Research suggests that teamwork can be strengthened through a network of cybersecurity champions, who are employees that promote good security practices and raise cybersecurity awareness at the team level. They serve as local points of contact for security issues within their teams or departments and support team leaders in establishing secure and expected behavior (Uchendu et al., 2021). These teamwork-based elements inform Question ID 12 in the survey.

Employee performance assessment is a critical domain influencing organizational culture, particularly in driving process improvements and facilitating organizational change. Assessments at the individual level help to identify areas requiring intervention and to promote desired behaviors. Their effectiveness can be enhanced by incorporating culturally sensitive questions and procedures into the assessment process (Gravina et al., 2021).

The assessment process should address both strengths and areas for improvement, acknowledging that employees often seek recognition for positive performance. Consequently, management should adopt a personalized strategy that links assessment outcomes to structured systems of reward and recognition (Vuong & Nguyen, 2022). Such an approach can bridge the gap between cybersecurity awareness and actual behavior, acting as an effective mechanism for reinforcing desired behaviors and discouraging undesired ones (Blythe et al., 2020). This dimension informs Questions 13 and 15 in the survey.

Further factors driving information security culture, as identified in the literature, include national culture (cf. da Veiga & Martins, 2017; Gcaza et al., 2015), while another important factor is employee motivation to engage in compliant behavior (D'Arcy & Greene, 2014). Additionally, the regulatory environment in which an organization operates also affects these cultural domains (Mokwetli & Zuva, 2018).

2.3 Survey

The survey was conducted in 2023 within a large energy retail organization that supplies electricity and distributed energy resources (DERs), such as smart meters, inverters, solar panels, and heat pumps, to both businesses and consumers across multiple European countries. Additionally, the organization maintains electric vehicle charging infrastructure. The company's Information Security Management System (ISMS) is based on ISO/IEC 27001.

Scale point	Description
1	Strongly disagree
2	Disagree
3	Neutral
4	Agree
5	Strongly agree

Table 2. Five-point Likert scale used in the survey

This company was selected because it is a key operator in the European energy retail sector and is within the scope of relevant European Union cybersecurity legislation, including the General Data Protection Regulation (GDPR) and the Directive on Security of Network and Information Systems (NIS 2). Invitations were sent to 2,075 employees, of whom 610 responded, resulting in a response rate of 29%. The survey comprised 18 questions, as shown in Table 1, using a 5-point Likert scale illustrated in Table 2.

Notably, five percent of the respondents hold a designated information security role within the company. Figure 1 shows the distribution of respondents based on their length of employment at the company.

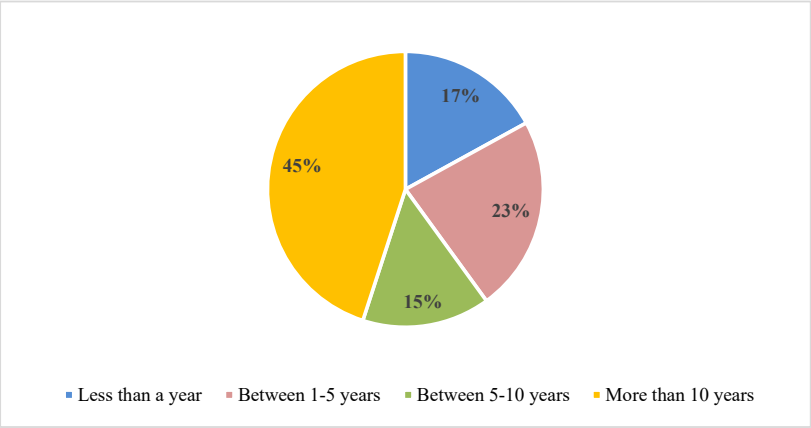

Figure 1. Length of employment of survey respondents

Histograms of the responses to each of the 18 survey questions, based on the 5-point Likert scale, are presented in Figure 2.

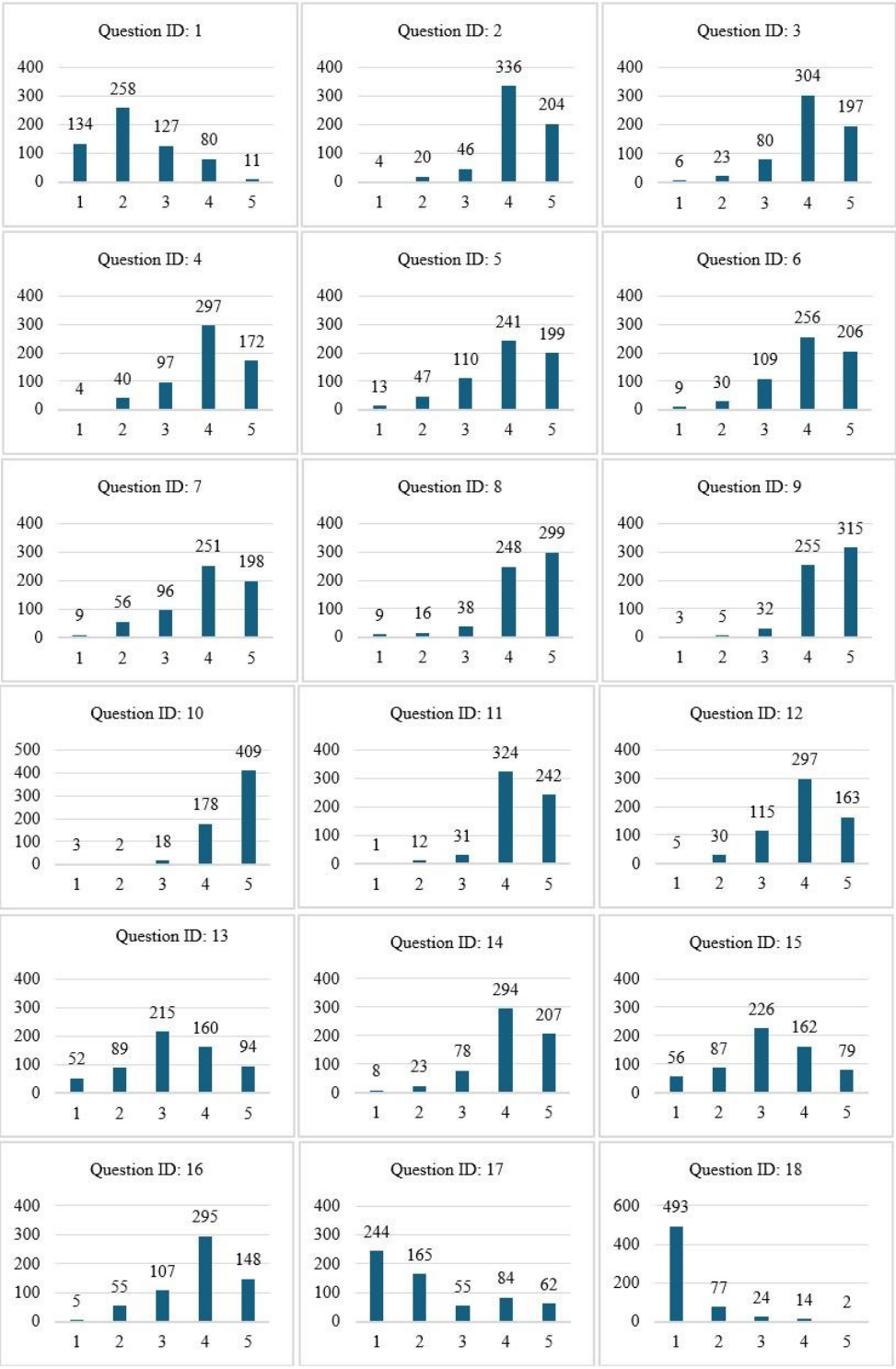

Figure 2. Histograms of survey questions

2.4 Exploratory factor analysis

Exploratory factor analysis (EFA) is a statistical technique used to identify underlying patterns in data without predefined assumptions. EFA supports decision-makers by reducing complexity, enabling them to focus on a smaller number of key factors rather than numerous individual parameters. EFA identifies the underlying factor correlations and structure through common factors, which are unobserved latent variables that affect multiple observed variables. It does this by grouping related measurements based on shared variance among observed variables (Shrestha, 2021).

In carrying out an EFA, several statistical and methodological considerations should be made. Best practices such as data inspection techniques, factor rotation, retention methods, and loading cutoff criteria, as recommended by Howard (2016), were followed in this work, as described below.

Before the analysis, the suitability of the data was tested by Bartlett's test of sphericity and the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy. Bartlett's test showed a significant result ($p < 0.001$), indicating that the data was applicable for factor analysis. The overall KMO measure was 0.89, suggesting that the sampling adequacy was high, and that the data was appropriate for factor analysis.

For the factor extraction method, the Maximum Likelihood estimation was chosen, as it is commonly used in EFA due to its ability to provide reliable estimates of factor loadings and model fit. Factor retention was determined using multiple different methods. The Velicer MAP (Minimum Average Partial) test recommended a two-factor approach, while parallel analysis indicated a three-factor solution. Based on these results and the interpretability of the factor structure, a three-factor solution was chosen for further analysis.

Regarding the rotation method, both oblique and orthogonal rotations were tested. The oblique rotation presumes that the factors are correlated, whereas orthogonal rotation

considers the factors to be uncorrelated. After testing both approaches, orthogonal Varimax rotation was chosen, as the resulting factors appeared to be uncorrelated and more easily interpretable.

Initially, all 18 variables were included in the factor analysis. However, some variables did not meet the sufficient criteria for factor loadings. Based on the recommendations from Howard (2016), variables were retained only if they met the following criteria:

(1) Factor loadings greater than 0.40 on their primary factor
(2) Loadings below 0.30 on alternative factors
(3) A difference greater than 0.20 between primary and alternative factor loadings

Variables that did not meet these criteria were excluded from the analysis. However, variables concerning survey questions 5 and 6 focusing on management engagement in information security were retained despite not fully meeting the loading criteria, as they were of particular focus to the study.

After removing the variables with weak loadings, Bartlett's test of sphericity was calculated again, with the result remaining significant ($p < 0.001$). The KMO measure was calculated at 0.69, which, although lower than the initial 0.89, was considered sufficient to continue the analysis. Given the clarity and interpretability of the resulting factor structure, three factors were retained, even though the initial factor retention analyses suggested retaining one or two factors.

After orthogonal Varimax rotation, the resulting factors were clear and interpretable. Each factor demonstrated satisfactory internal consistency, with Cronbach's alpha values surpassing the threshold of 0.7. Cronbach's alpha is a measure of how reliably the items in each factor work together. High Cronbach's alpha values demonstrate that the factors are reliable and have good internal consistency.

The final factor structure suggests that the data can be grouped into three distinct, yet internally consistent, dimensions. While the resulting factors were clear and interpretable, it is important to note that only 6 out of the 18 initial variables were retained in the final factor model. The six survey questions, together with their culture domains and loadings that form the three key factors, are presented in Table 3.

Key factor	Cronbach's alpha	Loading	Survey question	Culture domain
1	0.801	0.845	Question 5: My direct managers or supervisors have clearly explained the importance of security to me	Management engagement in information security
		0.695	Question 6: The management team of the company has conveyed the importance of security	Management engagement in information security
2	0.763	0.576	Question 13: Delivering on security responsibilities is considered in my overall performance assessment	Inclusion of information security in formal performance appraisal
		0.984	Question 15: In my team, good security behavior (i.e. doing the right thing) is rewarded	Inclusion of information security in formal performance appraisal
3	0.741	0.985	Question 9: I would report a cybersecurity issue if I noticed it. For example, a co-worker who continuously neglects security practices	Responsibility for information security reporting
		0.560	Question 10: If I accidentally caused a cybersecurity incident, I would immediately report it. For example, if I accidentally sent company information to the wrong recipient	Responsibility for information security reporting

Table 3. Survey questions, culture domains, and loadings

Factor scores for each participant were estimated using the regression method, resulting in continuous, standardized variables (mean = 0, standard deviation = 1) that represent their position on each latent dimension. These scores reflect the extent to which participants exhibit characteristics associated with each factor, with higher positive or negative values indicating stronger relationships.

Histograms of the estimated scores, presented in Figures 3, 4, and 5, illustrate the distribution of responses within the survey population. For example, a score of 1.75 indicates a strong positive association, while –2.5 reflects a strong negative association. Scores near zero suggest little to no relationship with the respective factor. These visualizations provide a clear summary of how individual responses relate to the underlying latent constructs identified in the analysis.

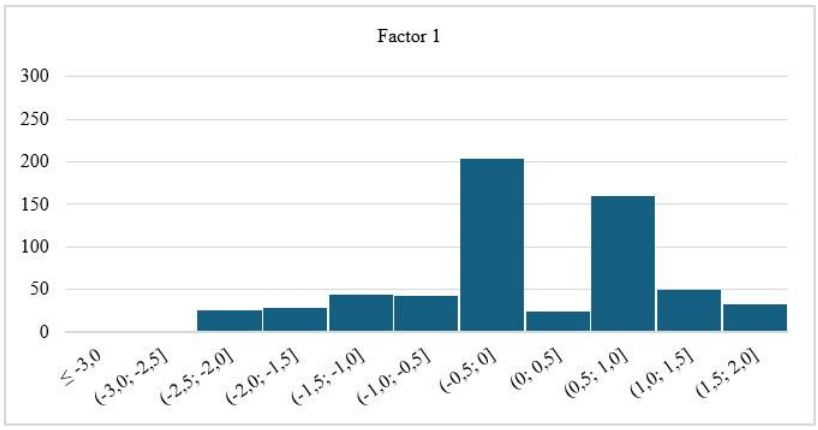

Figure 3. Factor score distribution for Factor 1

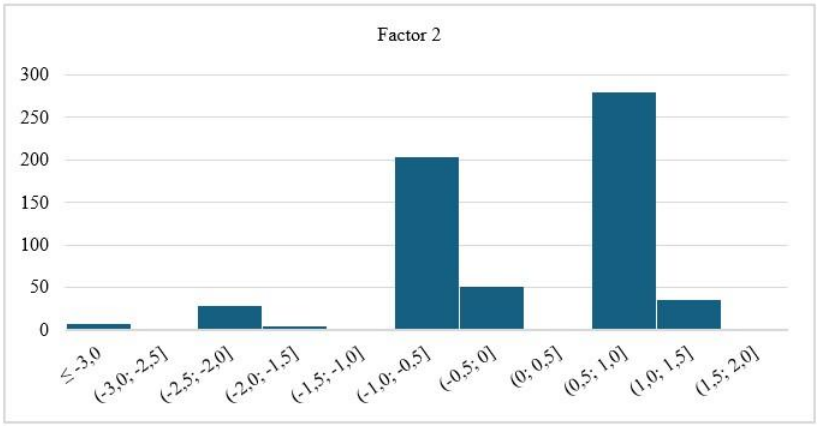

Figure 4. Factor score distribution for Factor 2

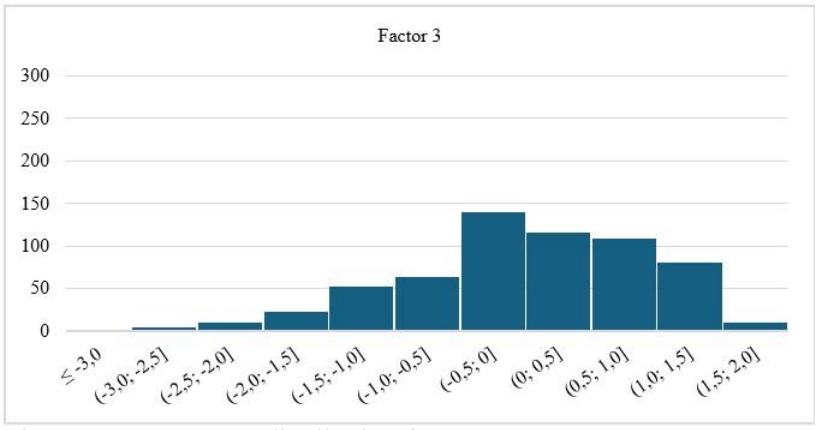

Figure 5. Factor score distribution for Factor 3

After factor scores were estimated using the regression method, Spearman's correlations were calculated between the 18 survey items and the derived factors. Spearman's correlation, which measures monotonic relationships, is appropriate for the

ordinal nature of the survey data. Figure 6 presents a correlation plot of the original survey variables. Correlation coefficients are visualized with color intensity and size corresponding to the strength of the associations. Deep blue indicates strong positive correlations, while deep red indicates strong negative correlations.

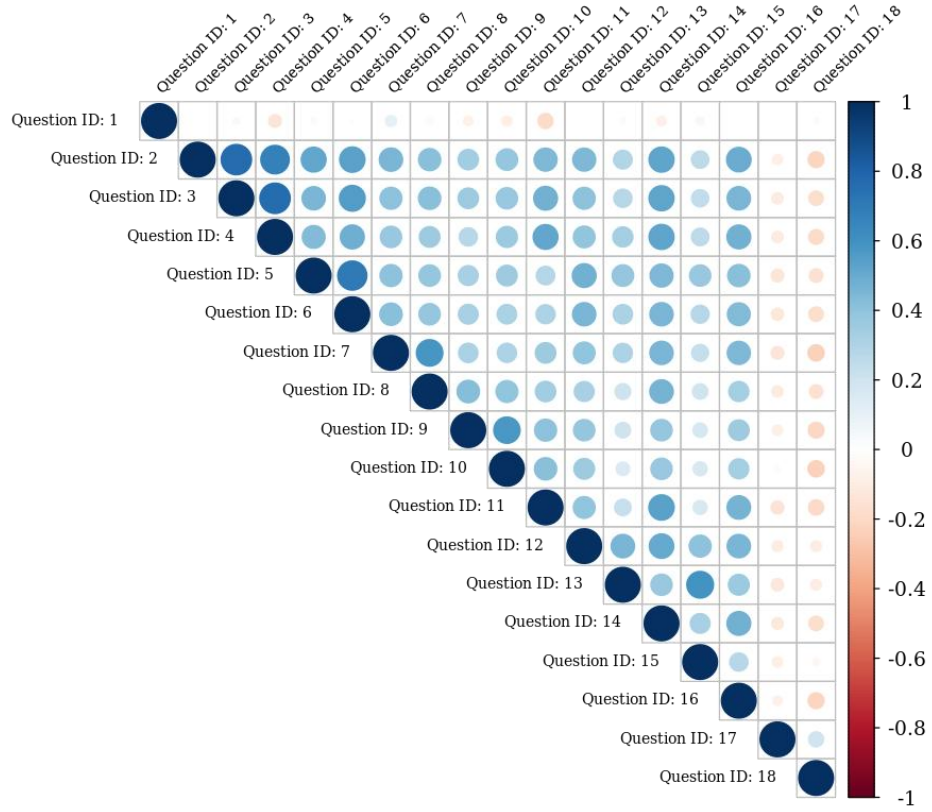

Figure 6. Correlation plot of the original survey variables

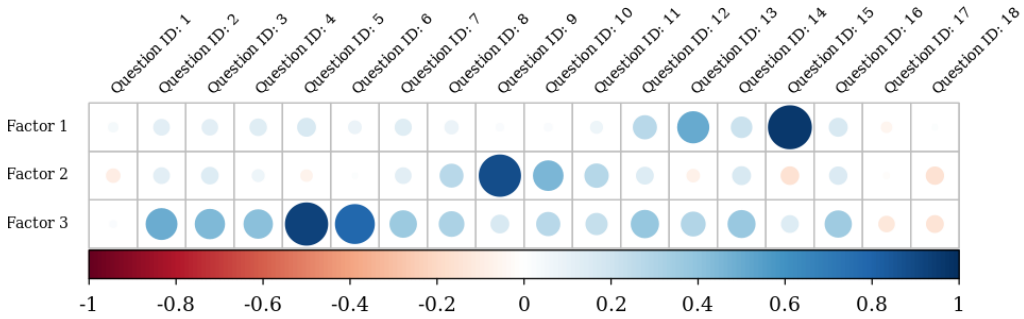

Figure 7. Correlation plot between original survey variables and factor scores

Figure 7 displays a similar correlation plot, illustrating the relationships between the original survey variables and the estimated factor scores. The visualization uses the same color and size coding to represent the strength and direction of these associations.

3. Results

This section addresses the research question by interpreting the exploratory factor analysis of the survey data, identifying the key factors that reinforce information security culture in European energy retail companies. The key factors, along with their factor components, are translated into more precise subfactors and, together with their corresponding survey questions, are summarized in Table 4.

The first key factor, "Management engagement in information security," consists of two subfactors: “ID 1.1. Top management engagement in information security” and “ID 2.1. Direct management engagement in information security.” Subfactor ID 1.1 highlights the role of senior leadership in setting the long-term strategic direction for information security, ensuring it is prioritized, resourced, and clearly communicated across the organization. Subfactor ID 2.1 emphasizes the responsibility of direct managers to translate high-level policies into daily practices and foster a security-conscious work environment at the team level. Together, these efforts strengthen the overall information security culture by aligning organizational objectives with employee awareness and accountability.

The second key factor, “Assessment and recognition of information security performance,” consists of two subfactors: “ID 2.1. Inclusion of information security responsibilities in employee performance evaluations” and “ID 2.2. Recognition and rewarding of positive information security behaviors.” Subfactor ID 2.1 highlights the integration of information security into employee performance assessments, ensuring accountability and reinforcing security as a personal responsibility and a core aspect of

daily operations. Subfactor ID 2.2 emphasizes the acknowledgement and rewarding of positive security practices, motivating employees to actively contribute to secure behaviors and embrace a proactive culture of information security risk mitigation.

Key factor	Factor component	Subfactor	Corresponding survey question	Culture at the individual level	Culture at the organizational level
(1) Management engagement in information security	Management engagement in information security	(1.1) Top management engagement in information security	Question 6: The management team of the company has conveyed the importance of security	Awareness	Security governance
	Management engagement in information security	(1.2) Direct management engagement in information security	Question 5: My direct managers or supervisors have clearly explained the importance of security to me	Awareness	Security governance
(2) Inclusion of information security in formal performance appraisal	Inclusion of information security in formal performance appraisal	(2.1) Inclusion of information security responsibilities in employee performance evaluations	Question 13: Delivering on security responsibilities is considered in my overall performance assessment	Awareness	Security governance
	Inclusion of information security in formal performance appraisal	(2.2) Recognition and rewarding of positive information security behaviors	Question 15: In my team, good security behavior (i.e. doing the right thing) is rewarded	Awareness	Security governance
(3) Assignment of responsibility for information security reporting	Assignment of responsibility for information security reporting	(3.1) Responsibility for information security risk reporting	Question 9: I would report a cybersecurity issue if I noticed it. For example, a co-worker who continuously neglects security practices	Behaviour	Access and trust
	Assignment of responsibility for information security reporting	(3.2) Responsibility for information security incident reporting	Question 10: If I accidentally caused a cybersecurity incident, I would immediately report it. For example, if I accidentally sent company information to the wrong recipient	Behaviour	Access and trust

Table 4. Key factors and their subfactors influencing information security culture

The third key factor, "Assignment of responsibility for information security reporting," consists of two subfactors: "ID 3.1. Responsibility for information security risk reporting" and "ID 3.2. Responsibility for information security incident reporting." Subfactor ID 3.1 highlights the importance of assigning staff members the responsibility to report any risks that threaten the confidentiality, integrity, or availability of assets and information. Subfactor ID 3.2 emphasizes the responsibility for reporting information security incidents that require immediate remedial action. Encouraging employee

vigilance in reporting risks and incidents enables early threat detection and timely mitigation. This proactive approach supports continuous learning, prevents recurrence, and strengthens the information security culture through openness and transparency in daily operations.

4. Discussion

This study identifies three interrelated factors that strengthen information security culture in European energy retail organizations: These include: (1) Management engagement in information security, (2) Inclusion of information security in formal performance appraisal and (3) Assignment of responsibility for information security reporting. These factors are best understood through the Cyber Security Culture Framework (Georgiadou et al., 2022), which emphasizes the interplay between organizational structures and individual behaviors in shaping holistic cybersecurity.

Management engagement is a critical driver of culture. Executives establish strategic direction and allocate resources, while direct managers translate these directives into actionable practices for teams and individuals. At the organizational level, this aligns with security governance, providing structures, policies, and processes to guide secure behavior. At the individual level, leadership involvement fosters awareness, ensuring employees understand the importance of security and internalize it in their daily work.

Assessment and recognition of performance reinforces the integration of security into everyday work. Incorporating security responsibilities into performance evaluations and acknowledging positive behavior signals that cybersecurity is integral to organizational operations. This links organizational-level governance with individual-level awareness, embedding security expectations into routine practices. Recognition and reward systems motivate employees, normalizing secure behavior and fostering a culture in which cybersecurity is valued rather than treated as an optional task.

Assignment of responsibility for reporting emphasizes individual accountability in identifying and addressing security risks. Encouraging employees to report risks and incidents promotes proactive behavior while supporting organizational trust and transparency. Clear reporting responsibilities enable early threat detection, timely remediation, and continuous improvement. Organizations that integrate reporting into daily workflows demonstrate a mature security culture, where employees feel empowered and accountable for protecting organizational assets.

Together, these factors show how organizational structures, governance, and policies interact with employee awareness, behavior, and competency to build a resilient, security-conscious culture. Aligning management engagement, performance assessment, and reporting responsibilities with both organizational and individual dimensions enables energy retail companies to foster proactive, consistent, and sustainable cybersecurity practices.

5. Conclusions

This study examines data from a European energy retail organization aligned with ISO/IEC 27001, fostering a security-aware culture (Putri et al., 2024; Folorunso et al., 2024). The sector plays a critical role in the energy value chain and in ensuring the resilience of essential societal functions. With rising cyber threats and increasingly stringent regulatory requirements, energy retail companies face growing pressure to protect the services they offer.

The results identify the key factors that drive the strengthening of information security culture. Although not a large-scale survey, the study provides insights into a typical utility organization operating in a regulated market. The analysis is based on survey responses from 610 employees, yielding a 29% response rate.

Exploratory Factor Analysis (EFA) of the survey data identified the underlying drivers shaping the organization's information security culture. The findings highlight the importance of commitment and communication from both executive and operational management at organizational and operational levels, ensuring alignment between organizational goals and information security priorities.

Furthermore, the results underscore the value of evaluating information security performance to embed security responsibilities into daily operations. Acknowledging compliant employee behavior and fostering a culture of cybersecurity risk and incident reporting support early detection and mitigation of potential issues, thereby strengthening the organization's overall cybersecurity resilience and culture.

5.1 Theoretical contributions

This study contributes to strengthening information security culture in energy retail organizations within the domain of IT Governance, Risk Management, and Compliance (IT-GRC), an area where research remains limited. Theoretically, it extends the research agenda of Gcaza and von Solms (2017) by examining factors influencing information security culture beyond the role of top management, a domain extensively studied in existing literature (cf. Reegård et al., 2019; Sharma & Aparicio, 2022).

In doing so, the study addresses Uchendu et al.'s (2021) call for further investigation into diverse drivers of information security culture. It examines elements such as incident and risk reporting (Ahola et al., 2024), employee performance assessment (Gravina et al., 2021), and the acknowledgement of compliant behavior (Vuong & Nguyen, 2022), all of which act as drivers in strengthening information security culture.

Furthermore, the study contributes theoretically through the application of the Cyber Security Culture Framework (Georgiadou et al., 2022). The framework provides a

holistic lens linking organizational and individual factors, thereby extending understanding of information security culture.

5.2 Practical implications

From a practical perspective, this study identifies three actionable key factors to strengthen information security culture in energy retail companies:

(1) Management engagement: Align executive communication and behavior with security priorities to foster organization-wide awareness and accountability. Top management should set a clear strategic direction, allocate necessary resources, and emphasize the importance of information security. Direct managers amplify these messages and embed required actions into daily team operations.

(2) Employee performance management: Integrate information security into existing employee performance management processes. Conduct regular assessments that evaluate and recognize compliant security behavior, reinforcing accountability. Apply targeted questions to clarify and maintain cybersecurity expectations aligned with organizational goals. Encourage positive behavior through systematic recognition and appraisal.

(3) Risk and incident reporting: Link performance evaluations and recognition directly to employees' responsibility for cybersecurity risk and incident reporting. This promotes proactive security practices, fosters a culture of openness, and ensures timely reporting and resolution of risks and incidents.

Additional consideration in large organizations, where central security teams cannot provide continuous team-level support, is to establish a formalized cybersecurity champions network. Champions would support and reinforce awareness by translating

security policies into practice, promoting compliant behavior, and facilitating timely risk and incident reporting (Alshaikh, 2020; Alshaikh & Adamson, 2021).

5.3 Limitations and future directions

This study has three key limitations. First, its findings are based on a single European energy retail organization, limiting generalizability across different cultural and regulatory contexts. Variations in leadership, risk perceptions, and security maturity may affect results, highlighting the need for further research in diverse settings to strengthen applicability.

Second, the study captures security culture at a single point in time, potentially overlooking changes due to evolving technology and emerging cybersecurity trends. Future research employing a longitudinal design is recommended to better understand the evolution of information security culture in energy retail organizations.

Third, from a methodological perspective, the study is grounded on self-reported survey data, which could be affected by biases like social desirability and respondent misinterpretation, potentially impacting the precision of the findings. In addition, the use of Exploratory Factor Analysis (EFA) introduces subjectivity through researcher decisions on factor extraction and rotation methods.

In this study, orthogonal Varimax rotation was applied to simplify the factor structure by assuming uncorrelated factors, enabling the interpretation of each factor as an independent influence on information security culture. Although this assumption can be questioned, since factors such as management engagement tend to be interrelated, orthogonal rotation remains a widely accepted approach in exploratory factor analysis. While oblique rotations allow for correlated factors, they can complicate interpretation and obscure the clear identification of distinct drivers.

Despite these limitations, this study addresses a significant research gap in the critical energy retail sector. Future studies positioned in the domain of IT-GRC research are encouraged to examine factors further strengthening the information security culture of energy retail organizations. Subsequent research could further explore the role of cybersecurity champions at the team level in supporting team leads by translating security policies into practice, promoting compliant behavior, and facilitating effective risk and incident reporting.

Ethics declaration: Ethical review and approval were not required for this study, as it was conducted as an anonymous internal survey within a private company in Germany. The research involved no sensitive personal data or vulnerable populations and was conducted in accordance with applicable national regulations and institutional policies governing internal organizational research.

References

Adeyinka, A. V., Moronkunbi, M. A., Oyedeji, O. C., Olusegun, P. V., & Samuel, S. A. (2024). The role of IT governance, risk, and compliance (IT GRC) in modern organizations. *International Journal of Latest Technology in Engineering, Management and Applied Science*, *13*(6), 44–50.

Ahola, K., Butavicius, M., McCormac, A., & Sturman, D. (2024). Hey "CSIRI", should I report this? Investigating the factors that influence employees to report cyber security incidents in the workplace. *Information and Computer Security*, *ahead-of-print*. https://doi.org/10.1108/ICS-11-2023-0214

AlHogail, A., & Mirza, A. (2014a). Information security culture: A definition and a literature review. In *2014 World Congress on Computer Applications and*

Information Systems (WCCAIS) (pp. 1–7). IEEE. https://doi.org/10.1109/WCCAIS.2014.6916579

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567–575. https://doi.org/10.1016/j.chb.2015.03.054

Ali, S., Green, P., & Parent, M. (2009). The role of a culture of compliance in information technology governance. In *GRCIS'09: Governance, Risk and Compliance* (Vol. 459). *Proceedings of the Second International Workshop on Governance, Risk and Compliance held in conjunction with CAiSE'09 Conference*, Amsterdam, The Netherlands, June 8, 2009.

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences, 11*(8), 3383. https://doi.org/10.3390/app11083383

Aljohani, T. M. (2024). Cyberattacks on energy infrastructures as modern war weapons – Part II: Gaps, standardization, and mitigation. *IEEE Technology and Society Magazine, 43*(2), 70–77. https://doi.org/10.1109/MTS.2024.3395697

Alnatheer, M. A. (2015). Information security culture critical success factors. In *2015 12th International Conference on Information Technology – New Generations* (pp. 731–735). IEEE. https://doi.org/10.1109/ITNG.2015.124

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Alshaikh, M., & Adamson, B. (2021). From awareness to influence: Toward a model for improving employees' security behaviour. *Personal and Ubiquitous Computing, 25*(4), 829–841. https://doi.org/10.1007/s00779-021-01551-2

Beerman, J., Berent, D., Falter, Z., & Bhunia, S. (2023). A review of Colonial Pipeline ransomware attack. In *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)* (pp. 8–15). IEEE. https://doi.org/10.1109/CCGridW59191.2023.00017

Blythe, J. M., Gray, A., & Collins, E. (2020). Human cyber risk management by security awareness professionals: Carrots or sticks to drive behavior change? In A. Moallem (Ed.), *HCI for cybersecurity, privacy and trust* (Vol. 12210, pp. 71–84). *Lecture Notes in Computer Science*. Springer. https://doi.org/10.1007/978-3-030-50309-3_6

Bronk, C., & Tikk-Ringas, E. (2013). The cyber attack on Saudi Aramco. *Survival, 55*(2), 81–96. https://doi.org/10.1080/00396338.2013.784468

Cuganesan, S., Steele, C., & Hart, A. (2018). How senior management and workplace norms influence information security attitudes and self-efficacy. *Behaviour & Information Technology, 37*(1), 50–65. https://doi.org/10.1080/0144929X.2017.1397193

da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002

da Veiga, A., & Martins, N. (2014). Information security culture: A comparative analysis of four assessments. In *Proceedings of the 8th European Conference on Information Management and Evaluation*. Ghent, Belgium. https://doi.org/10.13140/2.1.3221.8885

da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security, 70*, 72–94. https://doi.org/10.1016/j.cose.2017.05.002

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture – Perspectives from academia and industry. *Computers & Security, 92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security, 22*(5), 474–489. https://doi.org/10.1108/IMCS-08-2013-0057

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

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

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

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security, 22*(5), 410–430. https://doi.org/10.1108/IMCS-07-2013-0053

Ferrari, R. (2015). Writing narrative style literature reviews. *Medical Writing, 24*(4), 230–235. https://doi.org/10.1179/2047480615Z.000000000329

Folio III, J. C., Ross, A., Wolfe, I., & Weigel, N. A. (2025, February 25). Seeking harmony: CISA's proposed cyber reporting rules for critical infrastructure are an ambitious work in progress. *Cyber Security: A Peer-Reviewed Journal, 8*(3). https://doi.org/10.69554/JHEV8231

Folorunso, A., Mohammed, V., Wada, I., & Samuel, B. (2024). The impact of ISO security standards on enhancing cybersecurity posture in organizations. *World Journal of Advanced Research and Reviews, 24*(1), 2582–2595. https://doi.org/10.30574/wjarr.2024.24.1.3169

Gcaza, N., von Solms, R., & van Vuuren, J. J. (2015). An ontology for a national cyber-security culture environment. In *Proceedings of the International Symposium on Human Aspects of Information Security & Assurance (HAISA)* (pp. 1–10).

Gcaza, N., & von Solms, R. (2017). Cybersecurity culture: An ill-defined problem. In M. Bishop, L. Futcher, N. Miloslavskaya, & M. Theocharidou (Eds.), *Information security education for a global digital society* (Vol. 503, pp. 111–120). Springer. https://doi.org/10.1007/978-3-319-58553-6_9

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems, 62*(3), 452–462. https://doi.org/10.1080/08874417.2020.1845583

Gericke, A., Fill, H.-G., Karagiannis, D., & Winter, R. (2009). Situational method engineering for governance, risk, and compliance information systems. In *Proceedings of the 2009 ACM Symposium on Applied Computing* (pp. 1281–1287). https://doi.org/10.1145/1555619.1555651

Gorian, E. (2020). Singapore's Cybersecurity Act 2018: A new generation standard for critical information infrastructure protection. In D. Solovev (Ed.), *Smart technologies and innovations in design for control of technological processes and objects: Economy and production. FarEastCon 2018. Smart Innovation, Systems and Technologies* (Vol. 138, pp. 3–16). Springer. https://doi.org/10.1007/978-3-030-15577-3_1

Gravina, N., Nastasi, J., & Austin, J. (2021). Assessment of employee performance. *Journal of Organizational Behavior Management, 41*(2), 124–149. https://doi.org/10.1080/01608061.2020.1869136

Haber, E., & Zarsky, T. (2018). Cybersecurity for infrastructure: A critical analysis. *Florida State University Law Review, 44*(2). https://ir.law.fsu.edu/lr/vol44/iss2/3

Howard, M. C. (2016). A review of exploratory factor analysis decisions and overview of current practices: What we are doing and how can we improve? *International Journal of Human-Computer Interaction, 32*(1), 51–62. https://doi.org/10.1080/10447318.2015.1087664

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615–660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

Information Systems Audit and Control Association. (2018). *COBIT 2019 Framework: Governance and management objectives*. ISACA. https://www.isaca.org/resources/cobit

Ioannou, M., Stavrou, E., & Bada, M. (2019). Cybersecurity culture in computer security incident response teams: Investigating difficulties in communication and coordination. In *2019 International Conference on Cyber Security and Protection*

of Digital Services (Cyber Security) (pp. 1–4). IEEE. https://doi.org/10.1109/CyberSecPODS.2019.8885240

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).

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees' information security awareness in private and public organisations: A systematic literature review. *Computers & Security, 106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

Kör, B., & Metin, B. (2021). Understanding human aspects for an effective information security management implementation. *International Journal of Applied Decision Sciences, 14*(2), 105–122. https://doi.org/10.1504/IJADS.2021.113532

Lis, P., & Mendel, J. (2019). Cyberattacks on critical infrastructure: An economic perspective. *Economics and Business Review, 5*(19)(2), 24–47. https://doi.org/10.18559/ebr.2019.2.2

Lloyd-Jones, S. L. (2025). Ensuring digital resilience in Australia: From resilience to security in critical infrastructure protection. In D. Stephens, M. Stubbs, & S. White (Eds.), *Digital resilience* (pp. 103–120). Springer. https://doi.org/10.1007/978-981-97-9746-2_7

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

Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. (2017). A systematic literature review: Information security culture. In *Proceedings of the 2017 International Conference*

on Research and Innovation in Information Systems (ICRIIS) (pp. 1–6). IEEE. https://doi.org/10.1109/ICRIIS.2017.8002442

Mochinaga, D. (2024). Rising sun in the cyber domain: Japan's strategic shift toward active cyber defense. *The Pacific Review, 38*(2), 370–395. https://doi.org/10.1080/09512748.2024.2384447

Mokwetli, M., & Zuva, T. (2018). Adoption of the ICT security culture in SMMEs in the Gauteng Province, South Africa. In *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)* (pp. 1–7). IEEE. https://doi.org/10.1109/ICABCD.2018.8465139

Nasir, A., Arshah, R. A., Ab Hamid, M. R., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications, 44*, 12–22. https://doi.org/10.1016/j.jisa.2018.11.003

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

Nicho, M., Khan, S., & Rahman, M. S. M. K. (2017). Managing information security risk using integrated governance, risk, and compliance. In *2017 International Conference on Computer and Applications (ICCA)* (pp. 56–66). IEEE. https://doi.org/10.1109/COMAPP.2017.8079741

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (p. 156b). IEEE. https://doi.org/10.1109/HICSS.2007.206

Papazafeiropoulou, A., & Spanaki, K. (2015). Understanding governance, risk, and compliance information systems (GRC IS): The experts' view. *Information Systems Frontiers, 18*. https://doi.org/10.1007/s10796-015-9572-3

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

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

Putri, S. R. M., Bernandy, M. P., Aulia, C., Fikri, M. G. R., & Jasmine, J. (2024). Cyber security risk management practices: Insights from an ISO 27001 certified organization. *Journal of Digital Business and Innovation Management, 3*(2), 101–113. https://doi.org/10.26740/jdbim.v3i2

Reegård, K., Blackett, C., & Katta, V. (2019, September). The concept of cybersecurity culture. In *29th European Safety and Reliability Conference* (pp. 4036–4043). https://doi.org/10.3850/978-981-11-2724-3_0761-cd

Sanskriti, C., & Astitwa, B. (2018). Significance of ISO/IEC 27001 in the implementation of governance, risk and compliance. International Journal of Scientific Research in Network Security and Communication, 6(2), 30–33. https://doi.org/10.26438/ijsrnsc/v6i2.3033

Schein, E. H. (1996). Culture: The missing concept in organization studies. *Administrative Science Quarterly, 41*(2), 229–240. https://doi.org/10.2307/2393715

Sharma, S., & Aparicio, E. (2022). Organizational and team culture as antecedents of protection motivation among IT employees. *Computers & Security, 120*, 102774. https://doi.org/10.1016/j.cose.2022.102774

Sherif, E., Furnell, S., & Clarke, N. (2015). An identification of variables influencing the establishment of information security culture. In T. Tryfonas & I. Askoxylakis (Eds.), *Human aspects of information security, privacy, and trust* (pp. 477–486). Lecture Notes in Computer Science (Vol. 9190). Springer. https://doi.org/10.1007/978-3-319-20376-8_39

Schlaile, M. P., Bogner, K., & Muelder, L. (2021). It's more than complicated! Using organizational memetics to capture the complexity of organizational culture. *Journal of Business Research, 129*, 801–812. https://doi.org/10.1016/j.jbusres.2019.09.035

Schwartz, M. S. (2001). The nature of the relationship between corporate codes of ethics and behaviour. *Journal of Business Ethics, 32*, 247–262. https://doi.org/10.1023/A:1010787607771

Shrestha, N. (2021). Factor analysis as a tool for survey analysis. *American Journal of Applied Mathematics and Statistics, 9*(1), 4–11. https://doi.org/10.12691/ajams-9-1-2

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267–270. https://doi.org/10.1016/j.im.2008.12.007

Sommestad, T., Karlzén, H., & Hallberg, J. (2019). The Theory of Planned Behavior and information security policy compliance. *Journal of Computer Information Systems, 59*(4), 344–353. https://doi.org/10.1080/08874417.2017.1368421

Strupczewski, G. (2021). Defining cyber risk. *Safety Science, 135*, 105143. https://doi.org/10.1016/j.ssci.2020.105143

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002, and PCI DSS. *International Journal on Informatics Visualization, 4*(4), 4225–4230. https://doi.org/10.30630/joiv.4.4.482

Sullivan, J. E., & Kamensky, D. (2017). How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. *The Electricity Journal, 30*(3), 30–35. https://doi.org/10.1016/j.tej.2017.02.006

Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: A case study. *Information Technology and Management, 17*(2), 179–186. https://doi.org/10.1007/s10799-015-0252-2

Tolah, A., Furnell, S. M., & Papadaki, M. (2021). An empirical analysis of the information security culture key factors framework. *Computers & Security, 108*, 102354. https://doi.org/10.1016/j.cose.2021.102354

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

Valavanis, S. (2024). Understanding cybersecurity maturity in practice. *Journal of Information Systems, 38*(3), 1–5. https://doi.org/10.2308/ISYS-2024-026

Vicente, P., & da Silva, M. M. (2011). A business viewpoint for integrated IT governance, risk, and compliance. In *2011 IEEE World Congress on Services* (pp. 422–428). IEEE.

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. (2000). Information security - The third wave? *Computers & Security, 19*(7), 615–620. https://doi.org/10.1016/S0167-4048(00)07021-8

Von Solms, B. (2006). Information security – The fourth wave. *Computers & Security, 25*(3), 165–168. https://doi.org/10.1016/j.cose.2006.03.004

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

Vuong, T. D. N., & Nguyen, L. T. (2022). The key strategies for measuring employee performance in companies: A systematic review. *Sustainability, 14*(21), 14017. https://doi.org/10.3390/su142114017

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and information security awareness. *Computers & Security, 88*, 101640. https://doi.org/10.1016/j.cose.2019.101640

Yoo, C., Goo, J., & Rao, R. (2020). Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness. *MIS Quarterly, 44*(3), 907–931. https://doi.org/10.25300/MISQ/2020/15477

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

INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE
2024, VOL. 33, NO. 3, 285–306
https://doi.org/10.1080/19393555.2023.2270984

Information security failures identified and measured – ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis

M. Suorsa and P. Helo

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

ABSTRACT

This paper identifies the failures and impacts of information security, as well as the most effective controls to mitigate information security risks in organizations. Root cause analysis was conducted on all year 2020 GDPR penalty cases ($n = 81$) based on misconduct as defined in GDPR article 32: "security of processing." ISO/IEC 27001 controls were used as failure identifiers in the analysis. As a result, this study presents both the most frequent and most expensive information security failures and correspondingly ranks and presents the correlation of the controls observed in the analysis. From a theoretical perspective, our study contributes by bridging the gap between regulation and information security and introduces a statistical method to analyze the GDPR penalty cases, and provides previously unreported findings about information security failures and their respective solutions. From a practical perspective, the results of our study are useful for organizations which aspire to manage information security more effectively in order to prevent the most typical and expensive information security failures. Organizations, as well as auditors implementing and assuring the ISO 27001, may use our results as a guideline whereby controls should be applied and verified first in sequential order based on their impact and interdependence.

KEYWORDS

Information security; ISO 27001; GDPR; General Data Protection Regulation

1. Introduction

Information in its various forms is the most important asset of an organization; thus, failures in information security may not only threaten the integrity of organizations, but even their very existence (Gerber & von Solms, 2008). The primary objective of information security, the protecting of the confidentiality, integrity, and availability of information (Chapple et al., 2018), requires administration and governance (von Solms, 2006), whereby organizations' IT governance, risk management, and compliance function need to take decisions based on data-driven performance measurement metrics (Vaibhav, 2022).

International standardization frameworks play a necessary role in governing, assuring, and certifying effective information security in organizations (Siponen & Willison, 2009). The ISO/IEC 27001 is considered the de facto standard on how information security is managed, and it functions as the criterion for determining the quality, breadth, and depth of an organization's security controls (Calder & Gerard, 2013). Similar commonly used control frameworks are, e.g. The National Institute of Standards and Technology (NIST), Cyber Security Framework (CSF), and Control Objectives for Information and Related Technologies (COBIT) (Sulistyowati et al., 2020).

Legal aspects in terms of complying with information security and privacy regulation are becoming increasingly complex (Gerber & von Solms, 2008). The European Union General Data Protection Regulation (GDPR) aims to protect the privacy of EU citizens and consequently requires all organizations operating within the EU to have adequate control of information security (Regulation (EU) 2016/679). Violating the GDPR can lead to substantial financial penalties, and many have already been enforced (Ruohonen & Hjerppe, 2022).

Simultaneously, worldwide, many comparable regulatory frameworks, such as the GDPR, form a blueprint for how personal data may be protected and processed in a secure way. Developments

CONTACT M. Suorsa k83110@student.uwasa.fi School of Technology and Innovations, University of Vaasa, PB 700, Vaasa 65101, Finland

This article was originally published with errors, which have now been corrected in the online version. Please see Correction (http://dx.doi.org/10.1080/19393555.2024.2305508).

similar to GDPR are the California Consumer Privacy Act (CCPA) (cf. Thomas, 2020), Brazil's *Lei Geral de Proteçao de Dados* (LGPD) (cf. Macedo, 2021), India's Personal Data Protection Bill (PDPB) (cf. Deva & Suchithra, 2020), and Japan's Act on Protection of Personal Information (cf. Higashizawa & Aihara, 2017).

In order to govern information security and compliance with regulation, intelligence on information security failures and controls to effectively manage these failures are becoming ever more important (von Solms, 2006). The identification, ranking, and selecting of the most important information security controls is a fundamental step toward mitigating the risks and threats, but it is also a very tricky process, and has been a major management challenge for years (Tariq et al., 2020). Thus, more research efforts are needed to minimize the gap between regulation and information security (Dlamini et al., 2009).

Early GDPR penalties have already been studied (cf. Presthus & Sønslien, 2021). However, no studies have so far been conducted explicitly to analyze GDPR penalty cases with statistical methods to identify information security failures with control frameworks such as the ISO/IEC 27001:2013. Likewise, standardization frameworks and ISO 27001 have been utilized to construct capability maturity models to assess the information security posture of an organization (cf. Lopez-Leyva et al., 2020; Monev, 2020), but they do not rank the ISO/IEC 27001:2013 controls based on their impact and interdependence.

Assessing information security can be a complicated and costly operation, thus simple analysis method should be applied. Root cause analysis (RCA) is an effective method to achieve this goal (York et al., 2014). This study presents a novel method to analyze information security failures of organizations with GDPR penalties. In this paper, we apply the RCA method to measure information security failures as identified and measured by analyzing European Union General Data Protection Regulation (GDPR) penalty cases. All year 2020 penalties ($n = 81$) throughout the EU member countries based on the definition of misconduct in GDPR article 32, "security of processing," were analyzed and matched with ISO/IEC 27001:2013 standard controls. Our study matches the information security standard controls and the statistics from penalty cases, and provides previously unreported information about information security failure volumes and correlations within different industry domains.

The research problem of this paper is to identify and explore the failures and impacts of information security, as well as the most effective controls to mitigate the information security risks in organizations. More specific research questions are as follows:

RQ 1: What are the most frequent and most expensive information security failures corresponding to ISO 27001 controls?

RQ 2: How many information security failures corresponding to ISO 27001 controls typically exist in a GDPR penalty case?

RQ 3: How do the information security failures corresponding to ISO 27001 controls correlate?

RQ 4: Are there any industry type differences in information security failures and penalties?

The remainder of the paper is structured as follows. Section 2 presents a literature review and explores important aspects of GDPR, and positions the ISO/IEC 27001:2013 standard in an IT governance, risk management and compliance (IT-GRC) framework. Section 3 presents the material and methodology of the study. The results of the study are presented and discussed in section 4. Finally, section 5 concludes the paper, presenting theoretical and practical contributions as well as the limitations and future direction of the study.

2. Literature review

In this section, the important features and relevant literature of GDPR and ISO 27001 are presented and positioned in the IT governance, risk management and compliance (IT-GRC) framework. Table 1 presents the most relevant literature reviewed, bringing forth the research gap as well as positioning the IT-GRC as the overarching domain, governing information security with compliance with regulation and control frameworks.

Table 1. Literature review.

Authors	Category	Study design	Purpose
Selzer et al. (2021)	GDPR	Interviews	GDPR article 32 implementation impact
Ruohonen and Hjerppe (2022)	GDPR	GDPR penalty case document analysis with text mining technique	GDPR penalty impacts of individual articles
Presthus and Sønslien (2021)	GDPR	GDPR penalty case document analysis and interviews	GDPR penalty impacts of individual articles
Akhlaghpour et al. (2021)	GDPR	GDPR penalty case document analysis	GDPR compliance risk identification and categorization
Wolff and Atallah (2021)	GDPR	GDPR penalty case document analysis	GDPR violation type and penalty amount categorization
Wei et al. (2020)	GDPR	Privacy and security risk assessment tool design	Proposal of privacy and information security risk assessment tool
Osden and Lubbe (2009)	IT-GRC	Case study and interview	IT-GRC best practices identification
Nicho et al. (2017)	IT-GRC	Case study and interview	IT-GRC integration with standardization frameworks
Vaibhav (2021)	IT-GRC	Survey of literature	IT-GRC metrics identification
Sanskriti and Astitwa (2018)	IT-GRC	Literature review	IT-GRC and ISO 27001 relationship identification
Diamantopoulou et al. (2020)	ISO 27001	ISO 27001 controls and GDPR requirements analysis	ISO 27001 and GDPR synergies
Lopes et al. (2019)	ISO 27001	Survey	ISO 27001 as GDPR compliance facilitator
Shojaie et al. (2014)	ISO 27001	ISO 27001 analysis	ISO 27001 controls effectiveness categorization
Monev (2020)	ISO 27001	Information security maturity model design	Proposal of ISO 27001 based maturity model
Khajouei et al. (2017)	ISO 27001	Fuzzy analytic hierarchy process analysis	Information security controls ranking

2.1. The European Union General Data Protection Regulation

The European Union General Data Protection Regulation (GDPR) came into force in May 2018, and unified the diverse data protection laws throughout the EU into one regulation fit for purpose in the 21st century (Cornock, 2018). The main objective of GDPR is to safeguard the fundamental right of EU citizens to data protection and protection with respect to the processing of their personal data. GDPR lays out a wide variety of requirements as to how personal data may be processed by an organization, as well as granting individuals, also known as data subjects, many rights, which enable them to have more control over how their personal data is processed (Regulation (EU) 2016/679).

GDPR carries a paramount requirement about information security. The GDPR article 32, "security of processing," obliges organizations to implement technical and organizational measures to guarantee the adequate security of personal data. Article 32, however, does not require a specific set of such measures, because GDPR is technology neutral and grants a great deal of freedom in terms of how to realize compliance (Selzer et al., 2021). Providing only a minimum amount of guidance to meet the information security requirement, the regulation outlines examples and protection objectives, which include (Regulation (EU) 2016/679):

- The pseudonymization and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services
- The ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident
- A risk-based process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

The distinction between data processors and data controllers is important in GDPR. The data controller is the entity determining how personal data is used and is thus ultimately responsible for information security. For example, if a vendor hosts a website on behalf of an organization, the organization becomes the data controller, and the vendor will be the data processor (Hintze, 2018). When processing is outsourced to a processor, the controller may only contract such processors which are able to provide sufficient guarantees of adequate information security (Regulation (EU) 2016/679).

GDPR defines a data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed." As a consequence of a data breach, the data controller is obliged to make a timely report about it to the supervisory authority, as well as inform the data subjects of whether their right to privacy is significantly compromised (Regulation (EU) 2016/679).

The supervisory authorities acting in each EU member country have the task of ensuring compliance with the GDPR, and in order to fulfil this function they have various investigative and corrective powers. The most severe form of corrective power is administrative fines, where the maximum penalty is up to 20 million euros, or 4% of the total worldwide annual turnover (Regulation (EU) 2016/679). Penalties issued by the supervisory authorities are public information; thus GDPR enables transparency in cases of data breaches caused by information security failures throughout the European Union (Garrison & Hamilton, 2019).

Penalties are imposed depending on certain criteria such as the nature, gravity, and duration of the infringement, categories of personal data affected, the number of data subjects in scope, and the level of damage suffered by them, as well as aggravating or mitigating circumstances such as relevant previous infringements and the degree of cooperation with the supervisory authority. GDPR has allowed each EU member state to establish its own rules on the calculation of penalties and determine whether and to what extent penalties may be imposed on public organizations (Regulation (EU) 2016/679). The European Data Protection Board, which ensures the consistent application of GDPR, has published draft guidelines on the calculation of penalties to harmonize the methodology of the supervisory authorities (EDPB, 2022).

The relationship and interdependency between GDPR and information security is recognized in the literature (cf. Geko & Tjoa, 2018), but it is not entirely clear how information security frameworks can support compliance with GDPR (Serrado et al., 2020). However, models and tools have been proposed to assess the privacy risk, together with information security related risk, in order to assist organizations to select high-risk areas for further control actions (Wei et al., 2020).

Violations which led to GDPR penalties have already been explored and studied (cf. Ruohonen & Hjerppe, 2022, and Presthus & Sønslien, 2021). A study by Akhlaghpour et al. (2021) was conducted on 93 GDPR enforcement cases, which identified several risk categories and their associated mitigation measures. A similar study by Saemann et al. (2022) presented a work that analyzed and categorized 856 GDPR fines based on different violations, where it was found that one of the main drivers for GDPR penalties was the data subjects' complaints to authorities, or existing incidents which were a public concern.

The supervisory authorities' enforcement actions show that organizations fail to ensure adequate technical and organizational measures in implementing GDPR article 32 (Degli-Esposti & Ferrándiz, 2021). Previous studies show that penalties issued following the first 24 months after GDPR implementation were relatively conservative and did not reach the maximum threshold. Most of these early penalties were a response to privacy violations, but notably the majority of the larger fines were triggered by information security incidents, and, on average, information security violations led to relatively weightier fines than pure privacy violations (Wolff & Atallah, 2021).

Craddock (2022) argues that early GDPR fines were largely inconsistent, and proposes a methodology to forecast the amount of GDPR penalties in future, which will be much higher. Since the authorities are expected to get tougher with prosecutions (Barret, 2020), more research efforts are needed to analyze the impacts of GDPR (Hirvonen, 2022) to minimize the gap between regulation and information security (Dlamini et al., 2009).

2.2. IT governance, risk management and compliance framework

The information technology governance, risk management and compliance (IT-GRC) framework is derived from corporate governance, where the business focus is aligned with the IT management of an organization (Osden & Lubbe, 2009). The objective of IT-GRC is to implement effective management techniques with business strategies and IT, and also to manage industry standards and compliance with information security and regulatory requirements (Schlarman, 2009).

IT-GRC integrates and streamlines essential processes to manage the risks which threaten the confidentiality, integrity, and availability (CIA) of key operations of an organization (Nicho et al., 2017), while the primary focus of information security is, similarly, the commitment to ensuring the continuous CIA of information in an organization (Chapple et al., 2018). Information security is primarily risk management, and therefore it is

a fundamental element of IT-GRC (Wright, 2019), where governing decisions should be based on data-driven performance measurement metrics (Vaibhav, 2021).

Effective control frameworks are necessary when managing the information security risk within the organizational IT-GRC structure. A wide variety of information security standards to certify an organization, such as NIST and COBIT, are available, whereas the ISO/IEC 27001:2013 is one of the most facilitated standards (Dharmalingam et al., 2018; Sulistyowati et al., 2020) and recommended by the literature (cf. Brenner, 2007; Mayer & Smet, 2017). The relationship of ISO 27001 with successful IT-GRC is well recognized, because the standard encompasses all the necessary goals under its Information Security Management System (ISMS) to support an effective IT-GRC implementation (Sanskriti & Astitwa, 2018).

2.3. The ISO/IEC 27001:2013 in the ISO 27000 family of standards

The ISO/IEC 27000 family of standards is a numbered series of international information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The correct designation for the standard includes the ISO/IEC prefix, and a suffix which is their date of publication. The formal title of ISO 27001 standard is "Information technology – Security techniques – Information security management systems – Requirements" and is referred to simply as ISO 27001 (ISO/IEC 27001:2013).

The core of the ISO 27001 standard requires organizations to adopt a risk-based approach and provides a model for "establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) to protect the confidentiality, integrity and availability of information from threats and vulnerabilities." The standard requires establishing a risk assessment framework, identifying, analyzing, and evaluating risks, and finally selecting a risk treatment plan, which is the process of building the security controls to protect the organization's information assets (ISO/IEC 27001:2013).

ISO/IEC 27001:2013 controls are shown in Annex A, which first has 14 control clauses, each of which is identified with one or more control objectives, which are further served by a total of 114 controls (ISO/IEC 27001:2013). Table 2 presents an overview of ISO/IEC 27001:2013 Annex A.

The sequential ISO/IEC 27002:2013 standard, in turn, provides the best practices of how to implement an effective ISMS and guidelines for controls in ISO/IEC 27001:2013 Annex A, explaining how each control works and what its objective is (ISO/IEC 27002:2013). Both ISO 27001 and ISO 27002 are often used together, but only ISO 27001 is required for certifying an ISMS, so they are jointly referred to as the "common language of organizations around the world for information security" (Humphreys, 2011).

ISO 27002 was updated on February 15, 2022, and Annex A of ISO 27001 was aligned with those changes in the last quarter of 2022. In the new versions, the number of controls has decreased from 114 to 93, and these are placed in 4 sections instead of the previous 14. In the new versions, the security controls are divided into separate sections according to their specific type, which are organizational security controls ($n = 37$), personal safety controls ($n = 8$), physical security controls ($n = 14$), and technical safety controls ($n = 34$). In the new versions, there are 11 new controls. While none of the controls were deleted, some controls were merged together (ISO/IEC 27002:2022).

Notably, ISO/IEC 27701:2019 is an auxiliary standard to ISO 27001 and ISO 27002, and it specifies requirements and provides guidance for establishing, implementing, maintaining, and continually improving a Privacy Information Management System (PIMS). ISO 27701 is not mandatory for ISO 27001 certification, but it extends the information security requirements of ISO 27001 to take into account the protection of privacy and personally identifiable information, and provides guidance on how these requirements should be implemented ISO/IEC 27701:2019.

When placing ISO 27001 and GDPR side by side, it is clear that even though ISO 27001 and GDPR have different standpoints, they both apply a risk management approach to data. GDPR aims to mitigate the privacy risks of data subjects by placing various provisions on personal data processing,

Table 2. ISO/IEC 27001:2013 Annex A.

Control clause	Control objective	Number of controls
A.5 Information security policies	A.5.1 Management direction for information security	2
A.6 Organization of information security	A.6.1 Internal organization	5
	A.6.2 Mobile devices and teleworking	2
A.7 Human resource security	A.7.1 Prior to employment	2
	A.7.2 During employment	3
	A.7.3 Termination and change of employment	1
A.8 Asset management	A.8.1 Responsibility for assets	4
	A.8.2 Information classification	3
	A.8.3 Media handling	3
A.9 Access control	A.9.1 Business requirements of access control	2
	A.9.2 User access management	6
	A.9.3 User responsibilities	1
	A.9.4 System and application access control	5
A.10 Cryptography	A.10.1 Cryptographic controls	2
A.11 Physical and environmental security	A.11.1 Secure areas	6
	A.11.2 Equipment	9
A.12 Operations security	A.12.1 Operational procedures and responsibilities	4
	A.12.2 Protection from malware	1
	A.12.3 Backup	1
	A.12.4 Logging and monitoring	4
	A.12.5 Control of operational software	1
	A.12.6 Technical vulnerability management	2
	A.12.7 Information system audit considerations	1
A.13 Communications security	A.13.1 Network security management	3
	A.13.2 Information transfer	4
A.14 System acquisition, development and maintenance	A.14.1 Security requirements of information systems	3
	A.14.2 Security in development and support processes	9
	A.14.3 Test data	1
A.15 Supplier relationships	A.15.1 Information security in supplier relationships	3
	A.15.2 Supplier service delivery management	2
A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	7
A.17 Information security business continuity management	A.17.1 Information security continuity	3
	A.17.2 Redundancies	1
A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	5
	A.18.2 Information security reviews	3
Total		**114**

while ISO 27001 obliges organizations to adopt a continuously maintained ISMS (Diamantopoulou et al., 2020), which is a compliance facilitator to support the response of organizations to the security requirements of GDPR (Lopes et al., 2019).

As the ISO 27001 provides a deep-rooted history of development and best practices, it has been a basis for studies assessing the information security maturity and risks of organizations. However, these studies typically do not rank the ISO 27001 controls based on their impact or provide further input on how to improve the assessed maturity and risk levels (Anass et al., 2020).

For example, Monev (2020) proposes a methodology for performing information security maturity assessment solely based on ISO 27001 and ISO 27002. Another study by Nungky et al. (2022) proposes a situational awareness model to assess cybersecurity risks based on Annex A of ISO/IEC 27001:2013.

A study by Shojaie et al. (2014) classified the ISO/IEC 27001:2013 controls into categories which support organizations in evaluating and improving their ISMS performance, as well as providing understanding of relevant security flaws. Another study by Khajouei et al. (2017) provided a ranking of effective ISO/IEC 27001 control objectives in a single case organization. For similar studies, see, for example, Lopez-Leyva et al. (2020) and Makupi & Karume (2019). Furthermore, many of the proposed maturity models have been greatly influenced by the ISO 27001 (cf. Al-Matari et al., 2021; Bashofi & Salman, 2022).

3. Material and method

In this section the approach to gathering and analyzing the research data is described.

3.1. Material of the study

The publicly available data source for this study is the GDPR Enforcement Tracker, which is a freely

accessible website maintained by a global law firm, CMS. The database contains formal GDPR penalty case reports, which have been issued by the data protection authorities in EU member countries to organizations not complying with the regulation (GDPR Enforcement Tracker).

The database was searched with the year 2020, together with GDPR article 32 "security of processing," which resulted in 81 GDPR penalty case reports, where the penalty type was "insufficient technical and organizational measures to ensure information security." These GDPR penalty case reports formally describing and specifying information security failures accounted for the penalties issued to 81 different organizations. Out of the total of 81 GDPR penalty case reports, there were 25 cases which also included references to articles other than information security. The supervisory authorities issue penalties as a whole and do not distinguish the penalty amounts between failures in different quoted GDPR articles.

3.2. Methodology of the study

The method applied in the study was root cause analysis (RCA) to identify what caused the information security failures and what their impacts were. Root cause analysis as a method is a process which applies data collection, cause charting, root cause identification, and generation of recommendations. Only when root causes are determined can corrective measures that prevent future events of the type observed be specified (Rooney et al., 2004). The different RCA subtype methods can be summarized into the following three categories (York et al., 2014):

- Chart type RCAs, which are constructed in the style of a flow chart
- Tabular type RCAs, which are constructed in a table with predefined column headings and categories
- Graphical RCAs, which visualize the results in a bar graph or any graphical display of numerical data

Popular examples of chart type RCAs are the cause and effect diagram, current reality tree, and the cause and interrelationship diagram (Doggett, 2005). Tabular type RCAs are, for example, the 5 whys method (Card, 2016) and the Failure Modes and Effects Analysis (FMEA) (Paciarotti et al., 2014). Typical graphical RCAs are histograms and the pareto 80/20 method (York et al., 2014).

RCA as a methodology is challenged by the problem of "many hands," which means that the root causes cannot easily be pinpointed to a single individual or contributing factor responsible for the outcome or the solution that fixes the problem. RCA implies that there is only a single root cause, which often is not the case in a complex environment. RCAs also typically lack solutions to eliminate the root cause problems (Peerally et al., 2016).

The RCA method of this study is a mixture of tabular and graphical RCA types.

Each GDPR penalty case, with its respective information security failures corresponding to a specific failure identifier (ISO 27001 control), as well as the total penalty of the case, were mapped in a table. This table, which contained binary variables, enabled further analysis, and the graphical presentation of results is presented in Table 3.

This study was conducted before the new version of ISO/IEC 27001:2022 was published, and therefore the criteria of this analysis were the ISO/IEC 27001:2013 Annex A controls, which were used as root cause identifiers in each individual 81 GDPR penalty case.

There were 38 individual information security failures on the ISO 27001 control level, which included five failures that could not be matched

Table 3. RCA table example.

GDPR penalty case	Failure identifier a	Failure identifier b	Failure identifier c	Failure identifier n
Case 1	0	0	1	0
Case 2	1	0	1	1
Case 3	0	0	0	1
Case n	1	1	1	0

with any exact ISO 27001 control. These five failures were included in the scope of the analysis because they were specifically addressed by the supervisory authorities, and consequently were the cause of the issued penalties. In the presented results, these unmatched information security failures do not have the ISO number prefix, unlike the failures which were mapped to a specific ISO 27001 control. The 38 information security failures on the ISO 27001 control level were mapped to their respective 21 control objectives and further to their respective 12 control clauses, while the five unmatched failures were mapped within their own groups.

Penalty amount calculations for each individual information security failures were first conducted separately on the ISO 27001 control level. The total penalty amount of a single GDPR penalty case was divided by the number of information security failures that were observed in the case. For example, in a GDPR penalty case, where there were three observed information security failures and the total penalty was 600 euros, the cost of an individual failure was 200 euros. Next, the average was calculated for all information security failures, which became the penalty for each individual information security failure. Penalty amount calculations were further conducted separately on ISO 27001 control objectives and control clauses.

The 81 GDPR penalty cases were grouped to present the number of information security failures per case, which ranged from 1 to 13. The average penalty was calculated for each of these groups.

Information security failure correlations were calculated separately on ISO 27001 controls and further on their respective control objectives and control clauses. To emphasize their strategic significance, the ISO 27001 controls which had very strong (0.65 and above) correlation are presented in the results. After that, the fairly strong (0.35 and above) correlation of ISO 27001 control objectives and the correlation (0.3 and above) of ISO 27001 control clauses are presented in the results. P-values of the Pearson correlation were used, and results where the p-value was lower than 0.05 were considered statistically significant.

Finally, all the 81 GDPR penalty cases were grouped to present the penalty amounts and frequencies in different industry sectors.

4. Results and discussion

In this section the results of the analysis and answers to the research questions are presented. Both ISO/IEC 27002:2013 and ISO/IEC 27701:2019 standards are used for interpreting the results.

4.1. The most frequent information security failures

The top 10 most frequent information security failures corresponding to ISO 27001 controls are presented in Figure 1.

The most frequent ($n = 47$) failure is the lack of "A.9.4.1 Information access restriction."

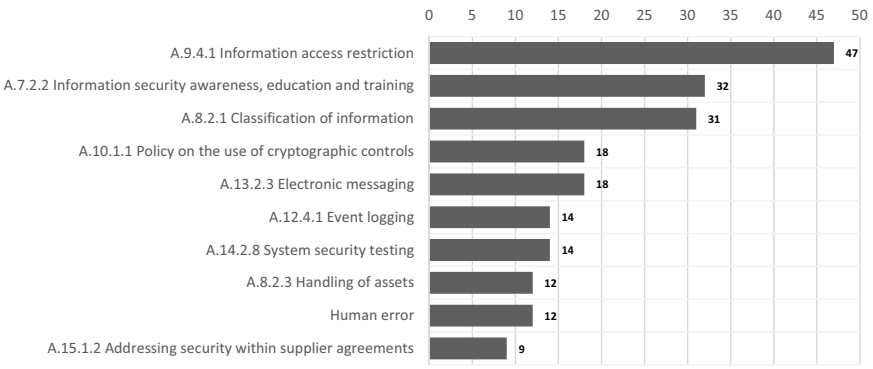

Figure 1. Top 10 most frequent information security failures corresponding to ISO 27001 controls.

Unauthorized access to organizational data was a very common cause of a data breach. Access restrictions such as controlling which data can be accessed by a particular user, controlling the access rights of users such as read, write, delete and execute, as well as limiting the information contained in outputs, should be based on individual business application requirements in accordance with the defined access controls policy (ISO/IEC 27002:2013).

The second most frequent failure ($n = 32$) are inadequacies in "A.7.2.2 Information security awareness, education and training." Shortcomings in this control can lead to a multitude of different problems if staff members do not know what is expected of them. Therefore, all employees of the organization and, where relevant, contractors, should receive appropriate awareness education and training and regular updates on organizational policies and instructions, as relevant to their job function (ISO/IEC 27002:2013). ISO 27701 further recommends ensuring that staff members are aware of the possible consequences of breaching privacy or security rules, especially those addressing the handling of personally identifiable information (ISO/IEC 27701:2019). ISO 27001 ISMS also requires organizations to determine the competence necessary for information security performance and ensure that employees have such competence through appropriate education, training, or experience (ISO/IEC 27001:2013).

The third most frequent failure ($n = 31$) is lack of "A.8.2.1 Classification of information." Information shall be classified in terms of legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification (ISO/IEC 27001:2013). The organization should mandate asset owners to follow the formal classifying scheme, which further specifies how the asset should be protected (ISO/IEC 27002:2013), while ISO 27701 further recommends taking personally identifiable information into consideration (ISO/IEC 27701:2019). This control applies to the GDPR article 32 requirement of having risk assessment conducted in order that adequate organizational and technical controls are further selected and implemented (Regulation (EU) 2016/679).

The fourth most frequent failure ($n = 18$) is lack of implementation of "A.10.1.1 Policy on the use of cryptographic controls," which is necessary to maximize the benefits of using cryptographic techniques and to avoid inappropriate or incorrect use. GDPR addresses encryption as a technique to secure personal data processing (Regulation (EU) 2016/679), although making a decision on whether a cryptographic solution is appropriate should be seen as part of the wider risk assessment process, which is used to determine whether a cryptographic control is appropriate and applied (ISO/IEC 27002:2013). ISO 27701 additionally guides the organization to provide information to the data subject regarding the circumstances in which it uses cryptography to protect personally identifiable information. The organization should also provide information to the data subject which can assist them in applying their own cryptographic protection (ISO/IEC 27701:2019).

The fifth most frequent failure (also $n = 18$) is lack of control in "A.13.2.3 Electronic messaging." Information involved in electronic messaging shall be appropriately protected (ISO/IEC 27001:2013). There are many types of electronic messaging such as e-mail, electronic data interchange, and social networking, which play a role in communications. Information security considerations should include, e.g. protecting messages from unauthorized access, or modification or denial of service in line with the risk-based classification scheme adopted by the organization (ISO/IEC 27002:2013).

The sixth most frequent failure ($n = 14$) is inadequate "A.12.4.1 Event logging." Many data breaches were caused by lack of tracing of user actions in systems. Therefore, event logs recording user activities, exceptions, faults, and information security events should be produced, kept, and regularly reviewed (ISO/IEC 27002:2013). ISO 27701 provides additional guidance by recommending a process to review the event logs, and where possible, event logs should specifically record user access to personally identifiable information (ISO/IEC 27701:2019).

The seventh most frequent failure (also $n = 14$) is lack of "A.14.2.8 System security testing," which is

important because GDPR requires regular testing and assessment of the effectiveness of measures for ensuring the security of processing (Regulation (EU) 2016/679). New and updated systems require thorough testing and verification during the development processes, including the preparation of detailed schedules of activities and test outputs under a range of conditions. The extent of testing should be in proportion to the importance and nature of the system (ISO/IEC 27002:2013), which once again refers to the need for having risk assessment conducted.

The eighth most frequent failure ($n = 12$) is lack of control in "A.8.2.3 Handling of assets." Procedures for handling an asset shall be developed and implemented in accordance with the information classification scheme adopted by the organization (ISO/IEC 27001:2013). The classification scheme used within the organization may not be equivalent to the schemes used by other organizations, which should be taken into account when information is transferred (ISO/IEC 27002:2013).

The ninth most frequent failure (also $n = 12$) is "Human error," which was not mapped to any specific ISO 27001 control. Human errors can be caused by insufficient information security awareness, education, and training. Human errors addressed by the supervisory authorities, however, also comprised pure accidents or the mistakes of well-educated staff members, leading to loss of confidentiality, integrity, or availability of information.

Finally, the tenth most frequent failure ($n = 9$) is lack of control in "A.15.1.2 Addressing security within supplier agreements", which is also required by GDPR (Regulation (EU) 2016/679). Supplier agreements should be established and documented to ensure that there is no misunderstanding between the organization and the supplier regarding both parties' obligations to fulfil relevant information security requirements. The agreements may vary considerably for different organizations and among different types of suppliers; thus, care should be taken to include all relevant information security risks and requirements (ISO/IEC 27002:2013). ISO 27701 further guides the organization to specify in agreements with suppliers whether personal data is processed and the minimum technical and organizational measures that the supplier needs to meet (ISO/IEC 27701:2019). All 38 information security failures corresponding to ISO 27001 controls are ranked based on their frequency and presented in Table 4.

A ranking of the most frequent information security failures corresponding to ISO 27001 control objectives is presented in Figure 2.

Information security failures corresponding to ISO 27001 control objectives reaching the threshold of 20 observations are explained here. The most frequent failure ($n = 58$) is the lack of "A.9.4

Table 4. Most frequent information security failures corresponding to ISO 27001 control.

ISO 27001 control	Failure frequency	Penalty
A.9.4.1 Information access restriction	47	225,065 €
A.7.2.2 Information security awareness, education, and training	32	40,598 €
A.8.2.1 Classification of information	31	603,400 €
A.10.1.1 Policy on the use of cryptographic controls	18	317,993 €
A.13.2.3 Electronic messaging	18	9,904 €
A.12.4.1 Event logging	14	309,183 €
A.14.2.8 System security testing	14	1,102,858 €
A.8.2.3 Handling of assets	12	69,025 €
Human error	12	149,951 €
A.15.1.2 Addressing security within supplier agreements	9	308,324 €
A.16.1.5 Response to information security incidents	9	223,375 €
Neglect of instructions	8	5,026 €
A.9.4.2 Secure log-on procedures	7	580,427 €
A.9.1.2 Access to networks and network services	6	297,929 €
A.16.1.4 Assessment of and decision on information security events	6	326,678 €
A.12.6.1 Management of technical vulnerabilities	5	42,019 €
A.9.4.3 Password management system	4	446,182 €
A.11.2.9 Clear desk and clear screen policy	4	11,685 €
A.12.1.4 Separation of development, testing, and operational environments	4	432,402 €
A.8.3.1 Management of removable media	3	10,483 €
A.14.1.2 Securing application services on public networks	3	569,592 €
A.16.1.1 Responsibilities and procedures	3	592,221 €
A.16.1.2 Reporting information security events	3	593,171 €
A.8.3.3 Physical media transfer	2	10,700 €
A.9.2.3 Management of privileged access rights	2	1,984,034 €
A.11.2.8 Unattended user equipment	2	5,250 €
A.12.2.1 Controls against malware	2	1,214,167 €
A.14.2.2 System change control procedures	2	11,714 €
A.14.2.7 Outsourced development	2	101,056 €
A.14.3.1 Protection of test data	2	21,463 €
A.5.1.1 Policies for information security	1	693 €
A.5.1.2 Review of the policies for information security	1	1,400 €
A.8.2.2 Labelling of information	1	7,083 €
A.11.1.5 Working in secure areas	1	7,083 €
A.12.1.2 Change management	1	2,272,222 €
Technical data integrity inconsistencies in systems leading to confidentiality breach	1	9,266,667 €
Personal data availability loss due to unspecified root cause	1	15,000 €
Usage of surveillance video cameras without proper authorization	1	1,667 €
Total	**294**	**22,187,689 €**

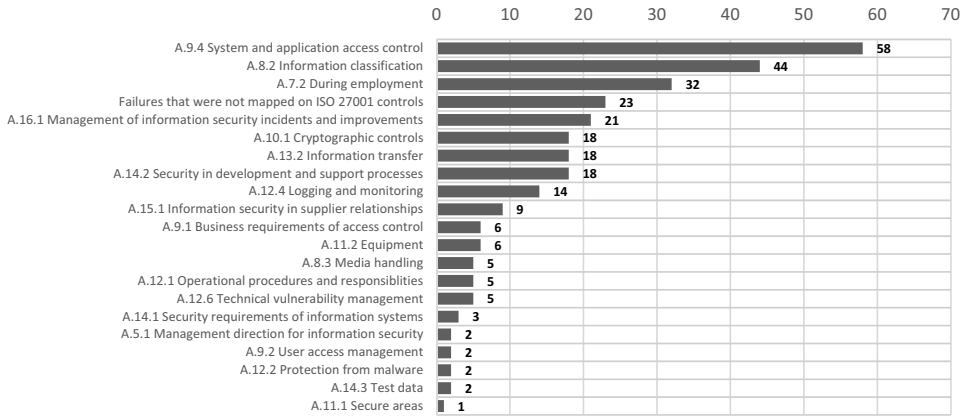

Figure 2. Most frequent information security failures corresponding to ISO 27001 control objectives.

System and application access control," where the objective is to prevent unauthorized access to systems and applications. The second most frequent failure ($n = 44$) is the lack of "A.8.2 Information classification," where the objective is to ensure that information receives an appropriate level of protection in accordance with its importance to the organization. The third most frequent failure ($n = 32$) is lack of controls "A.7.2 During employment," where the objective is to ensure that employees and contractors are aware of and fulfil their information security responsibilities after being recruited by an organization.

Fourth ($n = 23$) are information security failures that were not mapped on ISO 27001 controls, which form their own category. Most of these failures consist of pure human errors or the neglect of given instructions. The fifth most frequent failure ($n = 32$) is lack of "A.16.1 Management of information security incidents and improvements," where the objective is to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

A ranking of the most frequent information security failures corresponding to ISO 27001 control clauses is presented in Figure 3.

The most frequent information security failure corresponding to the ISO 27001 control clause is "A.9 Access control" ($n = 66$), followed by "A.8 Asset management" ($n = 49$) and "A.7 Human resource security" ($n = 32$). In conclusion, these results can be taken into account in organizations which aspire to manage information security

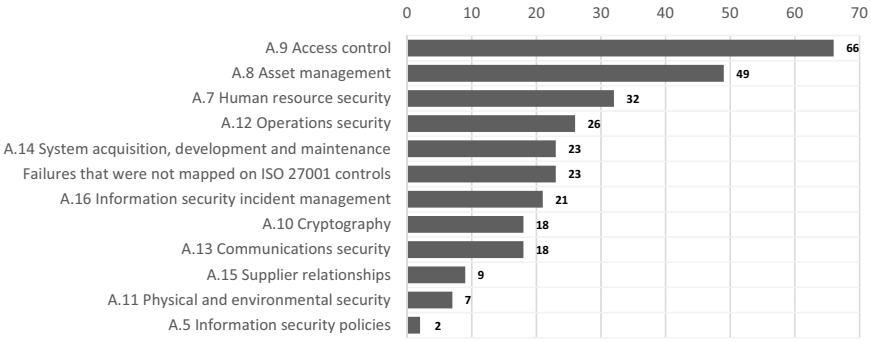

Figure 3. Most frequent information security failures corresponding to ISO 27001 control clauses.

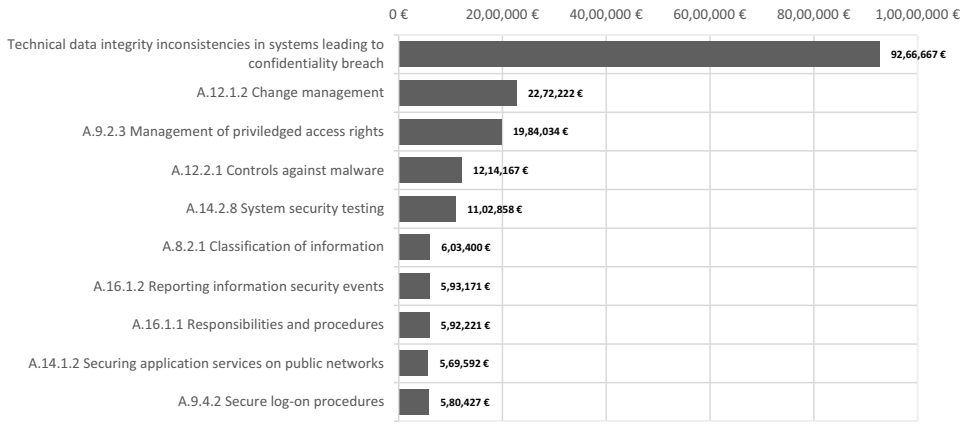

Figure 4. Top 10 most expensive information security failures corresponding to ISO 27001 controls.

more effectively to prevent the most typical failures by implementing controls based on their importance.

4.2. The most expensive information security failures

The top 10 most expensive information security failures corresponding to ISO 27001 controls are presented in Figure 4.

The most expensive failure (€ 9,266,667) was "Technical data integrity inconsistencies in systems leading to confidentiality breach." This failure was not mapped to any specific ISO 27001 control, and it was part of a penalty in a case where the total penalty was almost 28 million euros. In that penalty case there were only two other information security failures, which explains the high penalty amount for this failure, which can further be traced to controls and measuring how information systems shall be developed, tested, and maintained to protect data integrity and confidentiality.

The second most expensive failure (€ 2,272,222) was lack of control in "A.12.1.2 Change management." Inadequate control of changes to information security processing, facilities, and systems is a common cause of a data breach. Changes to the operational environment, especially when transferring a system from the development to operational stage, can impact the reliability of applications, and therefore formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes (ISO/IEC 27002:2013).

The third most expensive failure (€ 1,984,034) was inadequate "A.9.2.3 Management of privileged access rights." Inappropriate use of system administration privileges (any feature of an information system that enables the user to override system or application controls) is a major contributory factor to failures or breaches of systems. Thus, the allocation of privileged access rights should be controlled through a formal authorization process in accordance with the relevant access controls policy (ISO/IEC 27002:2013).

The fourth most expensive failure (€ 1,214,167) was inadequacies in "A.12.2.1 Controls against malware." Protection against malware shall be based on malware detection and repair software, information security awareness, and appropriate system access and change management controls (ISO/IEC 27001:2013). The use of malware detection and repair software as the sole malware control is not usually adequate and commonly needs to be accompanied by operating procedures that prevent the introduction of malware (ISO/IEC 27002:2013).

The fifth most expensive failure (€ 1,102,858) was inadequate "A.14.2.8 System security testing," followed by the sixth most expensive failure (€ 603,400) lack of control in "A.8.2.1 Classification of information," which were both present in the top 10 most frequent information security failures.

The seventh most expensive failure (€ 593,171) was inadequacy in "A.16.1.2 Reporting information

security events." All employees and contractors should be made aware of their responsibility to report information security events to the proper channels as quickly as possible (ISO/IEC 27002:2013).

The eighth most expensive failure (€ 592,221) was lack of "A.16.1.1 Responsibilities and procedures" concerning incident management, where management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents (ISO/IEC 27001:2013). If incidents are not reported, further investigated, and fixed, then incidents remain unaddressed, which consequently causes data breaches to become even more severe and more extensive. ISO 27701 further guides on establishing responsibilities and procedures for the identification and recording of breaches of personal data as well as notification to required parties, including the timing of such notifications and the disclosure to authorities (ISO/IEC 27701:2019), which is also required by GDPR (Regulation (EU) 2016/679).

The ninth most expensive failure (€ 569,592) was lack of control in "A.14.1.2 Securing application services on public networks." Applications accessible via public networks are subject to a range of network related threats, and therefore a detailed risk assessment and selection of controls is indispensable. The required controls often include cryptographic methods, authentication, and securing data transfer (ISO/IEC 27002:2013). ISO 27701 recommends encryption, specifically when personal data is transmitted over untrusted data transmission networks (ISO/IEC 27701:2019).

Finally, the tenth most expensive failure (€ 580,427) was lack of control in "A.9.4.2 Secure log-on procedures." The procedure for logging into a system or application should be designed to minimize the opportunity for unauthorized access, and thus a suitable authentication technique should be chosen to substantiate the claimed identity of a user. Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as cryptographic means, smart cards, or biometric means, should be used (ISO/IEC 27002:2013). ISO 27701 additionally guides the organization on providing the capability for secure log-on procedures for any user accounts under the data subjects control (ISO/IEC 27701:2019).

All 38 most expensive information security failures corresponding to ISO 27001 controls are presented in Table 5.

A ranking of the most expensive information security failures corresponding to ISO 27001 control objectives is presented in Figure 5.

Table 5. Most expensive information security failures corresponding to ISO 27001 control.

ISO 27001 control	Penalty	Failure frequency
Technical data quality inconsistencies in systems leading to confidentiality breach	9,266,667 €	1
A.12.1.2 Change management	2,272,222 €	1
A.9.2.3 Management of privileged access rights	1,984,034 €	2
A.12.2.1 Controls against malware	1,214,167 €	2
A.14.2.8 System security testing	1,102,858 €	14
A.8.2.1 Classification of information	603,400 €	31
A.16.1.2 Reporting information security events	593,171 €	3
A.16.1.1 Responsibilities and procedures	592,221 €	3
A.14.1.2 Securing application services on public networks	569,592 €	3
A.9.4.2 Secure log-on procedures	580,427 €	7
A.9.4.3 Password management system	446,182 €	4
A.12.1.4 Separation of development, testing, and operational environments	432,402 €	4
A.16.1.4 Assessment of and decision on information security events	326,678 €	6
A.10.1.1 Policy on the use of cryptographic controls	317,993 €	18
A.12.4.1 Event logging	309,183 €	14
A.15.1.2 Addressing security within supplier agreements	308,324 €	9
A.9.1.2 Access to networks and network services	297,929 €	6
A.9.4.1 Information access restriction	225,065 €	47
A.16.1.5 Response to information security incidents	223,375 €	9
Human error	149,951 €	12
A.14.2.7 Outsourced development	101,056 €	2
A.8.2.3 Handling of assets	69,025 €	12
A.12.6.1 Management of technical vulnerabilities	42,019 €	5
A.7.2.2 Information security awareness, education, and training	40,598 €	32
A.14.3.1 Protection of test data	21,463 €	2
Personal data availability loss due to unspecified root cause	15,000 €	1
A.14.2.2 System change control procedures	11,714 €	2
A.11.2.9 Clear desk and clear screen policy	11,685 €	4
A.8.3.3 Physical media transfer	10,700 €	2
A.8.3.1 Management of removable media	10,483 €	3
A.13.2.3 Electronic messaging	9,904 €	18
A.8.2.2 Labelling of information	7,083 €	1
A.11.1.5 Working in secure areas	7,083 €	1
A.11.2.8 Unattended user equipment	5,250 €	2
Neglect of instructions	5,026 €	8
Usage of surveillance video cameras without proper authorization	1,667 €	1
A.5.1.2 Review of the policies for information security	1,400 €	1
A.5.1.1 Policies for information security	693 €	1
Total	**22,187,689 €**	**294**

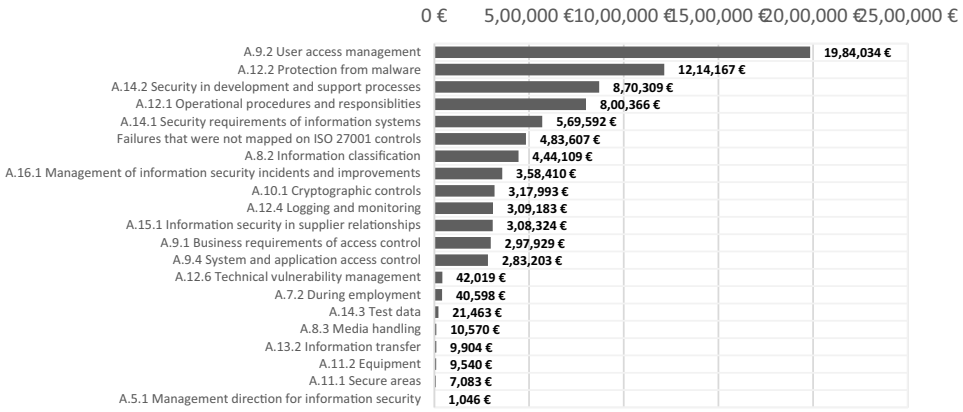

Figure 5. Most frequent information security failures corresponding to ISO 27001 control objectives.

Information security failures corresponding to ISO 27001 control objectives reaching the threshold of a 500,000 euro penalty are explained here. The most expensive failure (€ 1,984,934) was inadequate "A.9.2 User access management," where the objective is to ensure access for authorized users and to prevent unauthorized access to systems and services. The second most expensive failure (€ 1,214,167) was lack of "A.12.2 Protection from malware," where the objective is to ensure that information and information processing facilities are protected against malware. The third most expensive failure (€ 870,309) was lack of control in "A.14.2 Security in development and support processes," where the objective is to ensure that information security is designed and implemented within the whole development lifecycle of information systems.

The fourth most expensive failure (€ 800,366) was inadequate control in "A.12.1 Operational procedures and responsibilities," where the objective is to ensure correct and secure operations of information processing facilities. The fifth most expensive failure (€ 569,592) was lack of "A.14.1 Security requirements of information systems," where the objective is to ensure that information security is a fundamental element of information systems across their entire lifecycle.

A ranking of the most expensive information security failures corresponding to ISO 27001 control clauses is presented in Figure 6.

The most expensive information security failure corresponding to ISO 27001 control clause (€ 757,272) was inadequate "A.14 System acquisi-

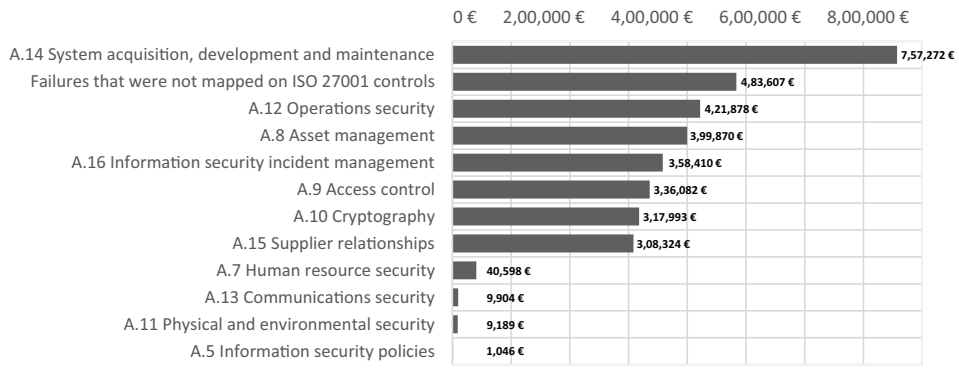

Figure 6. Most expensive information security failures corresponding to ISO 27001 control clauses.

Table 6. The amount of information security failures corresponding to ISO 27001 controls typically in a case.

Information security failures in a case	Number of cases	Percentage	Average penalty of the group
2	24	30%	317,341 €
3	20	25%	1,601,131 €
1	10	12%	€ 73350
5	7	9%	€ 41530
4	6	7%	€ 89991
8	4	5%	€ 102,150
7	3	4%	€ 4,241,867
9	3	4%	€ 7,363,433
6	2	2%	€ 147,420
12	1	1%	€ 85000
13	1	1%	€ 22046,000

tion, development and maintenance," followed by the category of failures (€ 483,607) which were not mapped specifically on any ISO 27001 control. The third most expensive failure was lack of control in "A.12 Operations security" (421,878 €), and in conclusion, these results can be taken into account in organizations which aim to manage information security more effectively to prevent the most expensive failures by implementing controls based on their importance.

4.3. The amount of information security failures in a GDPR penalty case

The amount of information security failures corresponding to ISO 27001 controls typically existing in GDPR penalty cases in the year 2020 is presented in Table 6.

The amount of information security failures ranges from 1 to 13 failures per GDPR penalty case. There are typically a low number of failures in a case. In 30% of the cases there were only 2 failures, and in 25% of the cases only 3 failures were observed, while single failure cases consisted of 12% of the cases analyzed. Cases where there were four or more failures comprised 33% of all the cases. Notably, there were only two cases with more than ten failures, and in the single case with the most observed – thirteen -information security failures, the penalty was over 22 million euros.

4.4. Information security failure correlations

Next, the results on how the information security failures corresponding to ISO 27001 controls correlate are presented. Information security failures

Table 7. Information security failure correlations corresponding to ISO 27001 controls.

ISO 27001 control 1	ISO 27001 control 2	Correlation	P-value
A.11.1.5 Working in secure areas	A.8.2.2. Labelling of information	1.00	***
A.8.3.3. Physical media transfer	A.8.3.1. Management of removable media	0.81	***
A.8.3.3 Physical media transfer	A.5.1.2. Review of the policies for information security	0.70	***
A.12.1.2 Change management	A.9.2.3 Management of privileged access rights	0.70	***
A.12.2.1 Controls against malware	A.12.1.2 Change management	0.70	***
A.16.1.2 Reporting information security events	A.16.1.1 Responsibilities and procedures	0.65	***
A.16.1.5 Response to information security incidents	A.16.1.4 Assessment of and decision on information security events	0.65	***

which have a fairly strong (0.30 and above) correlation, and which have statistical significance (p-value lower than 0.05) consist of a total of 61 observations. To highlight the strategic significance of these correlated controls, Table 7 presents the set of seven controls which have a very strong (0.65 and above) correlation.

The controls "A.11.1.5 Working in secure areas" and "A.8.2.2. Labelling of information" have a very strong correlation. In the analyzed cases, there were many data confidentiality breaches, where employees had not handled information within the organizations' physical premises in a secure way. Often, paper documents or other physical media containing sensitive personal data were transported outside of secure areas, and were later found in waste bins by complete outsiders. Therefore, a data labeling scheme, which further instructs on how information should be processed within the physical premises, is crucial. ISO 27701 additionally guides the organization on making their employees aware of the definition of personal data and how to recognize such information ISO/IEC 27701:2019.

The control "A.8.3.3. Physical media transfer" correlates with "A.8.3.1. Management of removable media" and "A.5.1.2. Review of the policies for information security." In many cases there were data breaches, where staff-members had lost unencrypted equipment or media containing sensitive information. Therefore, organizations should have a policy and instructions on how media containing information should be protected against unauthorized access, misuse, or corruption during transport, as well as procedures for the management of

removable media in accordance with the classification scheme adopted by the organization (ISO/IEC 27002:2013). ISO 27701 guides organizations on applying additional measures such as encryption to ensure that the removable media can only be accessed at the point of destination and not in transit (ISO/IEC 27701:2019).

The control "A.12.1.2 Change management" correlates with "A.9.2.3 Management of privileged access rights" and "A.12.2.1 Controls against malware." Changes to the organization, business processes, information processing facilities, and systems that affect information security should be managed together with privileged access rights administration because inappropriate system administration privileges are a major contributory factor to failures and system breaches. This has a connection to malware protection, because if malware is injected successfully to hack and misuse administrative accounts, the attackers gain the ability to make changes within IT systems, steal information, and possibly cover their tracks by disabling monitoring solutions and deleting system and security event logs (ISO/IEC 27002:2013).

A group of controls concerning incident management are naturally correlated together, because organizations need to have responsibilities and procedures in place to ensure a quick, effective, and orderly recognition of unexpected information security disruptions and incidents. Potential data breaches shall be reported through appropriate management channels as quickly as possible in order to be thoroughly assessed by competent personnel who are responsible for taking timely decisions on further actions.

Next, the results on how the information security failures corresponding to ISO 27001 control objectives correlate are presented. Information security failures, which have a fairly strong (0.30 and above) correlation, and which have statistical significance (p-value lower than 0.05), consist of a total of 19 observations. To foreground the strategic significance of these correlated controls, Table 8 presents the set of 11 controls which are above the 0.35 correlation rate.

Table 8. Information security failure correlations corresponding to ISO 27001 control objectives.

ISO 27001 control objective 1	ISO 27001 control objective 2	Correlation	p-value
A.9.2 User access management	A.12.1 Operational procedures and responsibilities	0.62	***
A.9.2 User access management	A.12.2 Protection from malware	0.49	***
A.11.2 Equipment	A.11.1 Secure areas	0.40	***
A.9.2 User access management	A.14.1 Security requirements of information systems	0.39	***
A.8.3 Media handling	A.5.1 Management direction for information security	0.39	***
A.9.4 System and application access control	A.13.2 Information transfer	−0.37	***
A.14.2 Security in development and support processes	A.12.4 Logging and monitoring	0.37	***
A.9.4 System and application access control	A.12.4 Logging and monitoring	0.36	***
A.12.1 Operational procedures and responsibilities	A.10.1 Cryptographic controls	0.36	***
A.9.2 User access management	A.12.4 Logging and monitoring	0.35	***
A.15.1 Information security in supplier relationships	A.14.1 Security requirements of information systems	0.35	***

The ISO 27001 security objective "A.9.2 User access management" correlates with many other security objectives. Unauthorized access to systems and services should be prevented in order that the secure operations of information processing facilities are assured. In addition, logging and monitoring are a crucial part of user access management in order that user specific actions can be traced, and this needs to be ensured within the whole development lifecycle of an information system according to control objective "A.14.2 Security in development and support processes."

The security control objectives "A.11.2 Equipment" and "A.11.1 Secure areas" correlate. So do the control objectives "A.8.3 Media handling" and "A.5.1 Management direction for information security." These correlation sets are explained by many data breaches being caused by inadequate organizational data labeling schemes, which should lead to further policies instructing how information within the premises of an organization needs to be handled, as well as how physical media and equipment need to be encrypted or otherwise adequately protected before they are transferred outside the organizational premises.

The security control objectives "A.9.4 System and application access control" and "A.13.2 Information transfer," however, have a negative

Table 9. Information security failure correlations corresponding to ISO 27001 control clauses.

ISO 27001 control clause 1	ISO 27001 control clause 2	Correlation	p-value
A.14 System acquisition, development and maintenance	A.12 Operations security	0.41	***
A.9 Access control	A.13 Communications security	−0.39	***
A.16 Information security incident management	A.12 Operations security	0.34	***
A.9 Access control	A.7 Human resource security	−0.32	***
A.7 Human resource security	A.13 Communications security	0.30	***

correlation. The prevention of unauthorized access to systems has no relation to procedures on how information should be transferred within an organization and with external entities.

In many GDPR penalty cases the failure was caused due to the supplier not being able to provide sufficient guarantees to supply adequate information security to the organization, which ultimately was the data controller. Therefore, security objective "A.15.1 Information security in supplier relationships" naturally correlates with "A.14.1 Security requirements of information systems."

Next, the results on how the information security failures corresponding to ISO 27001 control clauses correlate are presented. Information security failures, which have a fairly strong (0.30 and above) correlation and have statistical significance (p-value lower than 0.05) consist of a total of five observations. These are presented in Table 9.

The ISO 27001 control clause "A.12 Operations security" correlates with "A.14 System acquisition, development and maintenance" and "A.16 Information security incident management." It is natural that operations are closely connected to how systems security is continuously maintained, while efficient incident management should be at the heart of the daily business of an organization.

The control clause "A.9 Access control" has a negative correlation with "A.13 Communications security," which is explained by many GDPR penalty cases where failures in access control management do not coexist with failures regarding information transfer requirements.

However, the control clause "A.9 Access control" correlates with "A.7 Human resource security." Processes concerning employees hired by or departing from the organization, as well as staff-members changing positions within the organization, are governed by the HR function. Therefore, these processes should be aligned with access control management in order that new and obsolete, as well as the changing organizational roles of employees, correctly match with the access they have or should not have in systems and applications.

The control clause "A.7 Human resource security" also correlates with "A.13 Communications security." In the analyzed GDPR penalty cases, a multitude of data breaches took place in different electronic messaging channels such as e-mail, websites, and social media. These failures were caused by a lack of proper instructions and awareness training, which should be provided by the HR departments of an organization.

Table 10. GDPR penalties based on article 32 "security of processing" in the year 2020 per industry sector.

Industry sector	Total penalty	Average penalty	Number of cases
Media, Telecoms and Broadcasting	€ 42,050,136	€ 2,473,537	17
Transportation and Energy	€ 22,060,000	€ 4,412,000	5
Accommodation and Hospitality	€ 20,450,000	€ 20,450,000	1
Health Care	€ 7,166,987	€ 447,937	16
Industry and Commerce	€ 3,875,520	€ 276,823	14
Finance, Insurance and Consulting	€ 1,608,750	€ 201,094	8
Public Sector and Education	€ 1,606,300	€ 94,488	17
Real Estate	€ 20,600	€ 10,300	2
Employment	€ 15,000	€ 15,000	1
Total	**€ 98,853,293**	**€ 28,381,179**	**81**
Average	**€ 1,220,411**		

4.5. Industry type differences in information security failures and penalties

Table 10 presents the total and average GDPR penalties, as well as the number of cases based on article 32 "security of processing" in the year 2020 per industry sector.

In the year 2020 all the issued 81 GDPR penalties based on article 32 "Security of processing," where the penalty type was "insufficient technical and organizational measures to ensure information security," amounted to almost 100 million euros. The average of total penalties within all industry sectors was € 1,220,411.

The number of cases and total and average penalties vary significantly between different industry sectors. The largest amount of total

GDPR penalties was € 42,050,136, and the most issued 17 penalty cases were issued to the industry sector "Media, Telecoms and Broadcasting," which averaged a penalty of € 2,473,537 per case.

The industry sector "Public Sector and Education" was also issued with 17 penalty cases, but the total penalty was only € 1,606,300, averaging a penalty of € 94,488 per case. The results concerning public sector and education are affected by the inconsistent administrative fine calculation methods of the supervisory authorities. GDPR has allowed each EU member state to establish their own rules on penalties applicable to infringements, and to determine whether and to what extent administrative fines have been imposed on public organizations.

The industry sector "Accommodation and Hospitality" received the biggest average GDPR penalty of € 20,450,000 with its single penalty case. The industry sector "Transportation and Energy" had the second biggest average penalty of € 4,412,000, with five penalty cases issued. The industry sectors "Real estate" and "Employment" in turn received the smallest penalties, which are meager compared to other sectors.

5. Conclusions

This study has presented the most frequent and most expensive information security failures and consequently ranked the corresponding ISO 27001 controls that were used as failure identifiers in the analysis. The answer to RQ 1 is as follows: poor access control restriction and management of privileged access rights were very common causes of data confidentiality loss. The lack of implementing an appropriate information classification scheme was a cause of many different failures, because without risk assessments, further risk-based controls such as adequate cryptographic measures, suitable controls against malware, or proportionate system security development and testing could not be implemented. Failure to address security within supplier agreements was a common cause of incidents, as often there was a misunderstanding between the organization and supplier regarding both parties' obligations to fulfil the relevant information security requirements. Shortcomings in information security awareness, education, and training led to a multitude of different problems as staff members did not know what was expected of them.

This study further presented how many information security failures typically exist in a GDPR penalty case. The answer for RQ 2 is as follows: the amount of information security failures ranges from 1 to 13 failures per GDPR penalty case. There are typically a low number of failures in a case. In 30% of cases, there were only 2 failures, and in 25% of cases, 3 failures were observed, while single failure cases comprised 12% of the cases analyzed.

This study also presented how the observed information security failures correlate. The answer to RQ 3 is as follows: the top correlation was observed in inadequate organizational data-labeling schemes and lack of education on how employees should handle information assets within the premises of an organization. Several data confidentiality breaches were caused by careless staff members carrying documents containing sensitive personal data outside the facilities of an organization, which were later discovered in waste bins by complete outsiders. In many cases, staff-members had lost unencrypted equipment or media containing sensitive information during transfer. Inadequate control in information security incident management led to data breaches being unaddressed, which consequently caused failures to become more severe and more extensive; thus, a group of controls concerning incident management were naturally correlated together.

This study additionally presented insights into industry type differences in information security failures and penalties. The answer to RQ 4 is as follows: the number of cases, as well as total and average penalties, vary significantly between different industry sectors. The largest amount of total GDPR penalties (€ 42,050,136) and most issued (n = 17) penalty cases were experienced by the industry sector "Media, Telecoms and Broadcasting," while the industry sector "Employment" received only one (€ 15,000) penalty.

5.1. Theoretical and practical contributions

Firstly, our study contributes by bridging the gap between regulation and information security as presented by Dlamini et al. (2009). Secondly, our

study introduces a statistical method to analyze the GDPR penalty cases and provides previously unreported findings about information security failures and their respective solutions. Thirdly, our work expands on previous work by Ruohonen and Hjerppe (2022) and Presthus & Sønslien (2021) by further exploring early GDPR violations and sanctions from the year 2020.

From a practical perspective, our study provides input to the study of Vaibhav (2022) by providing data-driven performance measurement metrics to decision-making in information security governance. The results of our study are useful for organizations which aspire to manage information security more effectively in order to prevent the most typical and expensive information security failures by applying controls based on their importance and correlation. Organizations, as well as auditors implementing and assuring the ISO 27001, may use our results as a guideline whereby ISO 27001 controls should be applied and verified first in sequential order based on their impact and interdependence.

5.2. Limitations and future directions

There are three limitations in our study. Firstly, the quality of the GDPR penalty case reports written by the different supervisory authorities in each EU member county varies. The analyzed 81 penalty case reports do not always follow the same structure, and their length and level of precision differ. In some of the cases, the supervisory authority scrutinized the information security failures at a very detailed level. However, in other cases, the descriptions are comparatively limited; thus, it is possible that in these cases the underlying information security failure root causes were left undefined by the supervisory authority. In our study, however, only information security failures which were explicitly addressed in the penalty case reports were analyzed.

Secondly, the data source of our study, the GDPR Enforcement Tracker, may not be completely up to date. It is possible there were more than 81 GDPR penalty cases issued in the year 2020, which were not yet included in the database when this study was conducted. Additionally, organizations which were issued with a GDPR penalty may have lodged a court appeal, which may eventually alter the original supervisory authority decisions.

Thirdly, the penalty calculations of our study are not definitive. Even though all the 81 analyzed GDPR penalty cases can be categorized in the penalty type "insufficient technical and organizational measures to ensure information security," there were 25 cases which also included references to other GDPR articles, outside of the requirements considering information security. If a GDPR penalty is issued to an organization, the supervisory authorities administer penalties as a whole and do not separate the penalty amounts to address a specific article.

GDPR penalty cases are a fruitful and transparent ground to explore information security failures, their impacts, and respective solutions based on control frameworks. We encourage further research which would analyze GDPR penalty cases with the statistical methods we applied in our study with further versions of the ISO/IEC 27001 as well as with other similar standardization frameworks. It would also be constructive to analyze the readiness of organizations toward information security compliance with case study methods to generate more research hypotheses.

From a broader perspective, researchers and information security practitioners at other institutions are encouraged to use this study as a motivation to popularize the assessed and ranked information security controls in order to effectively manage the complex and challenging information security risks within organizational IT-GRC driven ISMS frameworks.

Disclosure statement

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

ORCID

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

References

Akhlaghpour, S., Hassandoust, F., Fatehi, F., Burton-Jones, A., & Hynd, A. (2021). Learning from enforcement cases to manage GDPR risks. *MIS Quarterly Executive*, *20*(3), 199–218. https://doi.org/10.17705/2msqe.00049

Al-Matari, O. M. M., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2021). Integrated framework for

cybersecurity auditing. *Information Security Journal: A Global Perspective*, *30*(4), 189–204. https://doi.org/10.1080/19393555.2020.1834649

Anass, R., Assoul, S., Ouazzani, T. K., & Roudies, O. (2020). Information and cyber security maturity models: A systematic literature review. *Information and Computer Security*, *28*(4), 627–644. https://doi.org/10.1108/ICS-03-2019-0039

Bashofi, I., & Salman, M. (2022), Cybersecurity maturity assessment design using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002, *2022 IEEE International Conference on Cybernetics and Computational Intelligence* pp. 58–62, https://doi.org/10.1109/CyberneticsCom55287.2022.9865640.

Brenner, J. (2007). ISO 27001 risk management and compliance. *Risk Management*, *54*(24), 28–29.

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.

Card, A. J. (2016). The problem with '5 whys'. *BMJ Quality & Safety*, *26*(8), 671–677. https://doi.org/10.1136/bmjqs-2016-005849

Chapple, M., Stewart, J. M., & Gibson, D. (2018). Security governance through principles and policies. In J. T. Parker, B. Sipes, & D. Seidl (Eds.), *Certified information systems security professional official study guide* (pp. 1–48). Sybex.

Cornock, M. (2018). General data protection regulation (GDPR) and implications for research. *Maturitas*, *111*, A1–A2. https://doi.org/10.1016/j.maturitas.2018.01.017

Craddock, P. (2022). Comparing past GDPR fines to future ones under EDPB's guidelines, and making a GDPR fine calculator. *Computer Law Review International*, *23*(5), 136–140. https://doi.org/10.9785/cri-2022-230503

Degli-Esposti, S., & Ferrándiz, E. M. (2021). After the GDPR: Cybersecurity is the elephant in the artificial intelligence room. *European Business Law Review*, *32*(1), 1–24. https://doi.org/10.54648/eulr2021001

Deva, P. M., & Suchithra, M. C. (2020). The personal data protection bill, 2018: India's regulatory journey towards a comprehensive data protection law. *International Journal of Law and Information Technology*, *28*(1), 1–19. https://doi.org/10.1093/ijlit/eaaa003

Dharmalingam, R., Shivasankarappa, A., & Neelamegam, A. (2018). A novel approach for optimizing governance, risk management and compliance for enterprise information security using DEMATEL and FoM. *Procedia Computer Science*, *134*, 365–370. https://doi.org/10.1016/j.procs.2018.07.197

Diamantopoulou, V., Tsohou, A., & Karyda, M. (2020). From ISO/IEC27001: 2013 and ISO/IEC27002: 2013 to GDPR compliance controls. *Information and Computer Security*, *28*(4), 645–662. https://doi.org/10.1108/ICS-01-2020-0004

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security*, *28*(3–4), 189–198. https://doi.org/10.1016/j.cose.2008.11.007

Doggett, M. A. (2005). Root cause analysis: A framework for tool selection. *Quality Management Journal*, *12*(4), 34–45. https://doi.org/10.1080/10686967.2005.11919269

EDPB. (2022). *Guidelines 04/2022 on the calculation of administrative fines under the GDPR*. European Data Protection Board. https://edpb.europa.eu/system/files/202205/edpb_guidelines_042022_calculationofadministrativefines_en.pdf

Garrison, C., & Hamilton, C. (2019). A comparative analysis of the EU GDPR to the US's breach notifications. *Information & Communications Technology Law*, *28*(1), 99–114. https://doi.org/10.1080/13600834.2019.1571473

GDPR enforcement Tracker. *CMS*. https://www.enforcementtracker.com

Geko, M., & Tjoa, S. (2018). An ontology capturing the interdependence of the General data protection Regulation (GDPR) and information security. *CECC 2018: Proceedings of the Central European Cybersecurity Conference 2018*, 1–6 https://doi.org/10.1145/3277570.3277590

Gerber, M., & von Solms, R. (2008). Information security requirements – interpreting the legal aspects. *Computers and Security*, *27*(5–6), 124–135. https://doi.org/10.1016/j.cose.2008.07.009

Higashizawa, N., & Aihara, Y. (2017). Data privacy protection of personal information versus usage of big data: Introduction of the recent amendment to the act on the protection of personal information (Japan). *Defense Counsel Journal*, *84*(4), 1–15.

Hintze, M. (2018). Data controllers, data processors, and the growing use of connected products in the enterprise: Managing risks, understanding benefits, and complying with the GDPR. *Journal of Internet Law*, *22*(2), 17–31. https://doi.org/10.2139/ssrn.3192721

Hirvonen, P. (2022). A review of GDPR impacts on information security. *Proceedings of the 26th Pacific Asia Conference on Information Systems*, 83. https://aisel.aisnet.org/pacis2022/83

Humphreys, E. (2011). Information security management system standards. *Datenschutz und Datensicherheit - DuD*, *35*(1), 7–11. https://doi.org/10.1007/s11623-011-0004-3

ISO/IEC 27001. 2013, information Technology – security techniques – information security management systems – requirements*International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)*.

ISO/IEC 27002. 2013, information Technology – security techniques – code of practice for information security controls. *International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)*.

ISO/IEC 27002. 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, 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)*.

Khajouei, H., Kazemi, M., & Moosavirad, S. H. (2017). Ranking information security controls by using fuzzy analytic hierarchy process. *Information Systems and eBusiness Management*, *15*(1), 1–19. https://doi.org/10.1007/s10257-016-0306-y

Lopes, M. I., Guarda, T., & Oliveira, P. (2019). Implementation of ISO 27001 standards as GDPR compliance facilitator.

Journal of Information Systems Engineering and Management, *4*(2). https://doi.org/10.29333/jisem/5888

Lopez-Leyva, J. A., Kanter-Ramirez, C. A., & Morales-Martinez, J. P. (2020), Customized diagnostic tool for the security maturity level of the enterprise information based on ISO/IEC 27001, *2020 8th International Conference in Software Engineering Research and Innovation*, 147–153, https://doi.org/10.1109/CONISOFT50191.2020.00030.

Macedo, A. C. (2021). Some thoughts about the intersection between data protection and competition law: A view from Brazil. *Journal of Antitrust Enforcement*, *9*(2), 197–202. https://doi.org/10.1093/jaenfo/jnab007

Makupi, D., & Karume, S. (2019). Towards an information security maturity model for universities based on ISO 27001. *Journal of Humanities & Social Sciences*, *3*(6), 241–245. https://doi.org/10.24940/theijbm/2019/v7/i6/BM1906-038

Mayer, N., & Smet, D. D. (2017). Systematic literature review and ISO standards analysis to integrate IT governance and security risk management. *International Journal for Infonomics*, *10*(1). https://doi.org/10.20533/IJI.1742.4712.2017.0154

Monev, V. (2020). Organisational information security maturity assessment based on ISO 27001 and ISO 27002. *2020 International Conference on Information Technologies (InfoTech)*. https://doi.org/10.1109/InfoTech49733.2020.9211066

Nicho, M., Khan, S., & Rahman, M. S. M. K. (2017), Managing information security risk using integrated governance risk and compliance. *2017 International Conference on Computer and Applications (ICCA)*,Doha, United Arab Emirates.

Nungky, A. C., Ramli, K., Anak Agung, P. R., & Teddy, S. G. (2022). Information security risk assessment using situational awareness frameworks and application tools. *Risks*, *10*(8), 165. https://doi.org/10.3390/risks10080165

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

Paciarotti, C., Mazzuto, G., & D'Ettorre, D. (2014). A revised FMEA application to the quality control management. *International Journal of Quality & Reliability Management*, *31*(7), 788–810. https://doi.org/10.1108/IJQRM-02-2013-0028

Peerally, M. F., Carr, S., Waring, J., & Dixon-Woods, M. (2016). The problem with root cause analysis. *BMJ Quality & Safety*, *26*(5), 417–422. https://doi.org/10.1136/bmjqs-2016-005511

Presthus, W., & Sønslien, K. F. (2021). An analysis of violations and sanctions following the GDPR. *International Journal of Information Systems & Project Management*, *9*(1), 38–53. https://doi.org/10.12821/ijispm090102

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, and repealing directive 95/46/EC (General data protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj

Rooney, J. J., Lee, N., & Van den, H. (2004). Root cause analysis for beginners. *Quality Progress*, *37*(7), 45–53.

Ruohonen, J., & Hjerppe, K. (2022). The GDPR enforcement fines at a glance. *Information Systems*, *106*, 101876. https://doi.org/10.1016/j.is.2021.101876

Saemann, M., Theis, D., Urban, T., & Degeling, M. (2022). Investigating GDPR fines in the light of data flows. *Proceedings on Privacy Enhancing Technologies*, *2022*(4), 314–331. https://doi.org/10.56553/popets-2022-0111

Sanskriti, C., & Astitwa, B. (2018). Significance of ISO/IEC 27001 in the implementation of governance, risk and compliance. *International Journal of Scientific Research in Network Security and Communication*, *6*(2), 30–33. https://doi.org/10.26438/ijsrnsc/v6i2.3033

Schlarman, S. (2009). What ITIL can teach IT-GRC. *The EDP Audit, Control, and Security Newsletter*, *40*(2), 8–18. https://doi.org/10.1080/07366980903340012

Selzer, A., Woods, D., & Böhme, R. (2021). Practitioners' corner · an economic analysis of appropriateness under article 32 GDPR. *European Data Protection Law Review*, *7*(3), 456–470. https://doi.org/10.21552/edpl/2021/3/15

Serrado, J., Pereira, R. F., Mira da Silva, M., & Scalabrin, B. I. (2020). Information security frameworks for assisting GDPR compliance in banking industry. *Digital Policy, Regulation & Governance*, *22*(3), 227–244. https://doi.org/10.1108/DPRG-02-2020-0019

Shojaie, B., Federrath, H., & Saberi, I. (2014), Evaluating the effectiveness of ISO 27001: 2013 based on annex a. *IEEE, 2014 Ninth International Conference on Availability, Reliability and Security*. https://doi.org/10.1109/ARES.2014.41

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267–270. https://doi.org/10.1016/j.im.2008.12.007

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *International Journal on Informatics Visualization*, *4*(4), 4225–4230. https://doi.org/10.30630/joiv.4.4.482

Tariq, M. T., Tayyaba, S., Ali, M. T., Safraz, M. S., De La-Hoz-Franco, E., Butt, S. A., Starcangelo, V., & Rad, D. V. (2020). Combination of AHP and TOPSIS methods for the ranking of information security controls to overcome its obstructions under fuzzy environment. *Journal of Intelligent & Fuzzy Systems*, *38*(5), 6075–6088. https://doi.org/10.3233/JIFS-179692

Thomas, I. (2020). Getting ready for the California consumer privacy act: Building on general data protection regulation preparedness. *Applied Marketing Analytics*, *5*(3), 210–222.

Vaibhav, A. (2022). Information security governance metrics: A survey and taxonomy. *Information Security Journal: A Global Perspective*, *31*(4), 466–478. https://doi.org/10.1080/19393555.2021.1922786

von Solms, B. (2006). Information security – the fourth wave. *Computers and Security*, *25*(3), 165–168. https://doi.org/10.1016/j.cose.2006.03.004

Wei, Y. C., Wu, W. C., Lai, G. H., & Chu, Y. (2020). pISRA: Privacy considered information security risk assessment model. *The Journal of Supercomputing*, *76*(3), 1468–1481. https://doi.org/10.1007/s11227-018-2371-0

Wolff, J., & Atallah, N. (2021). Early GDPR penalties: Analysis of implementation and fines through May 2020. *Journal of Information Policy*, *11*, 63–103. https://doi.org/10.5325/jinfopoli.11.2021.0063

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

York, D., Jin, K., Song, Q., & Li, H. (2014). Practical root cause analysis using cause mapping. *Proceedings of the International MultiConference of Engineers and Computer Scientists 2014, IMECS 2014*, Hong Kong.

INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE
2024, VOL. 33, NO. 4, 454
https://doi.org/10.1080/19393555.2024.2305508

Correction

Article title: Information security failures identified and measured – ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis
Authors: Suorsa. M., & Helo, P.
Journal: *Information Security Journal: A Global Perspective*
DOI: 10.1080/19393555.2023.2270984

For the above mentioned article, incorrect version of Figure 5 and legend has been used during the original publication. The revised figure and legend are incorporated and the article is re-published online.

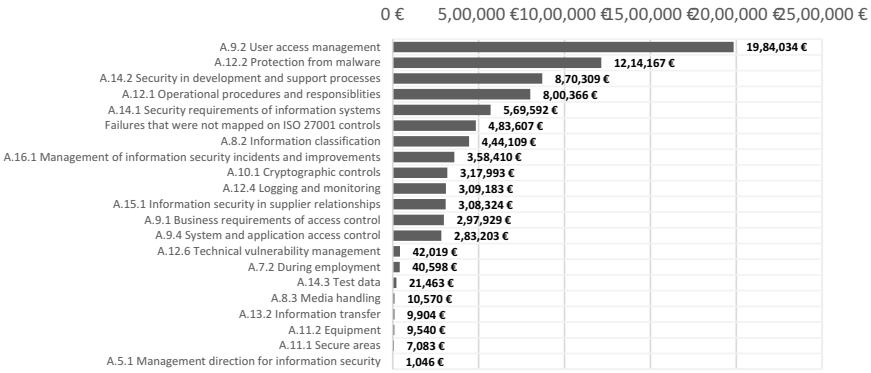

Figure 5. Most frequent information security failures corresponding to ISO 27001 control objectives.

Information Security Failures Measured and ISO/IEC 27001:2022 Controls Ranked by General Data Protection Regulation Penalty Analysis

Mikko Suorsa
School of Technology and Innovations
University of Vaasa
Vaasa, Finland
ORCiD: 0000-0002-1649-4223

Petri Helo
School of Technology and Innovations
University of Vaasa
Vaasa, Finland
ORCiD: 0000-0002-0501-2727

Abstract—**Selecting the most important information security controls is a critical and difficult process. Therefore, the decision-making on how to manage risks and threats has to be supported with data-driven performance measurement metrics. This paper identifies and explores the failures and impacts of information security, as well as the most effective controls to mitigate information security risks in organizations. The method of the study was root cause analysis. All year 2020 GDPR penalty cases (n=81) based on misconduct, as defined in GDPR Article 32: "Security of processing" were matched with ISO/IEC 27001:2022 controls, which were used as failure identifiers in the analysis. As a result, the study presents both, the top 10 most frequent and the top 10 most expensive information security failures corresponding to ISO/IEC 27001:2022 controls. Furthermore, the study also illustrates the correlation of these controls.**

Keywords— Information security, IT risk management, IT compliance, ISO/IEC 27001:2022, General Data Protection Regulation, GDPR

I. INTRODUCTION

Information is a very important asset of any organization and therefore failures in information security may not only threaten the success of organizations but also their continuation [1]. However, the identification, ranking, and decision to apply the most crucial information security controls to mitigate the risks and threats is a difficult process and a major management challenge [2].

Regulatory requirements to comply with information security and privacy laws are becoming more demanding [1]. The EU General Data Protection Regulation (GDPR) protects the privacy of EU citizens and requires all organizations operating within the EU to have sufficient control of information security [3]. Breaching the rules of GDPR can lead to large monetary sanctions, and enforcement actions have already been commenced [4].

Intelligence on information security failures and controls to effectively manage these failures is becoming an ever more important process in order to govern information security and compliance with regulations [5]. Therefore, optimized decisions when selecting the most impactful security controls should be based on data-driven performance measurement metrics [6].

International standardization frameworks play a decisive role in governing, assuring, and certifying effective information security in organizations [7], whereas the ISO 27001 is one of the most applied standards for determining the organization's information security controls [8]. However, studies ranking the most important ISO 27001 controls based on their effectiveness are limited.

Responses need to be undertaken on security controls to sufficiently meet the data protection requirements [9]; thus, research efforts are necessary to reduce the gap between regulation and information security [10]. GDPR penalties have already been studied and explored, but no studies have so far been conducted to specifically analyze GDPR penalty cases using statistical methods to identify information security failures with certification frameworks such as the controls in the ISO/IEC 27001:2022.

This leads us to the research problem of this paper, which is to identify and explore the failures and impacts of information security, as well as the most effective controls to mitigate information security risks in organizations. We address this problem with the research question: ***What are the most frequent and most expensive information security failures corresponding to ISO/IEC 27001:2022 controls, and what is their correlation?***

In this paper, we measure information security failures by performing a root cause analysis on European Union GDPR penalty case documents. All year 2020 penalties (n=81) throughout the EU member countries based on the definition of misconduct in GDPR Article 32, "Security of processing", were analyzed and matched with the ISO/IEC 27001:2013 standard controls, and after the new version ISO/IEC 27001:2022 was published, the results were migrated to correspond with the new version of the standard.

II. BACKGROUND

A. The EU General Data Protection Regulation

The EU GDPR came into force in May 2018, and the primary objective of the law is to protect the fundamental right of EU citizens to data protection and the processing of their personal data. GDPR brings forth a significant requirement for information security. The GDPR Article 32, "Security of processing", forces organizations to apply technical and organizational measures to ensure the adequate security of personal data [3].

The supervisory authorities acting in each EU member country have the task of ensuring compliance with the GDPR, and in order to fulfil this operation they have various investigative and corrective powers. The most stringent form of corrective power is administrative fines, where the maximum penalty is up to 20 million euros, or 4 % of the total global annual turnover of an organization [3].

GDPR sanctions are issued depending on certain criteria such as the nature, gravity, and duration of the infringement, which furthermore becomes public information, and therefore GDPR enables transparency in cases of data breaches caused by information security failures throughout the European Union member countries [11]. GDPR has allowed each EU

member state to enact its own rules on judging whether and to what extent penalties may be enforced on public organizations [3]. However, the European Data Protection Board, which ensures the consistent application of GDPR, has published guidelines to harmonize the different methodologies of the various national supervisory authorities.

Infringements which led to GDPR sanctions have already been explored and studied. One study analyzed GDPR penalty case documents with data mining techniques for the purpose of providing information about the penalty impacts of individual articles of GDPR [4]. GDPR penalty case documents have also been analyzed to provide intelligence about GDPR violation types and penalty amount categorizations [12] [13].

GDPR penalty case document analyses have also been supplemented with interviews to provide information about GDPR compliance risk identification and its respective mitigation [14]. However, no studies have so far been performed to specifically analyze GDPR penalty cases using statistical methods to identify information security failures with certification frameworks such as the controls in the new ISO/IEC 27001:2022.

B. The ISO/IEC 27001:2022 in the ISO 27000 family of standards

The ISO/IEC 27000 family of standards is a numbered series of international information security standards. The foundation of the ISO 27001:2022 standard requires organizations to apply an information security management system (ISMS) in order to implement a risk-based approach and administer controls to protect the confidentiality, integrity, and availability of information from threats and vulnerabilities. The ISO 27001:2022 controls are located in Annex A [15].

The sequential ISO/IEC 27002:2022 standard provides the guidelines for the implementation of an effective ISMS and controls in ISO 27001 Annex A [16]. ISO/IEC 27701:2019 is an auxiliary standard for both ISO 27001 and ISO 27002, and it defines requirements and further guidance for establishing a privacy information management system. It broadens the information security requirements of ISO 27001 to take into its scope the protection of privacy and personally identifiable information (PII) and provides direction on how these requirements should be implemented [17].

Studies show that the ISO 27001 framework has been used to construct information security risk assessment methodologies [18] and capability maturity model assessment tools for organizations [19]. One study categorized the ISO 27001 controls based on their effectiveness in supporting organizations in evaluating and enhancing their ISMS conduct, as well as providing an understanding of relevant security flaws [20].

Another study was conducted with fuzzy analytic hierarchy process to rank the ISO 27001 controls [21], while further studies analyzed the GDPR requirement with ISO 27001 controls to provide information about their synergies [9], and it was suggested that ISO 27001 is a GDPR compliance facilitator [22]. However, currently, there are no studies addressing information security failures with statistical methods based on the new ISO/IEC 27001:2022 controls and further ranking them.

III. MATERIAL AND METHOD

A. Material search

The publicly available data source for this study is the GDPR Enforcement Tracker, which is a freely accessible website maintained by a global law firm, CMS. The database accommodates reports on cases of formal GDPR penalties issued by the authorities in EU member countries to organizations not adhering to the law [23].

The database was searched through filtering by the year 2020, together with GDPR Article 32 "Security of processing", which resulted in 81 GDPR penalty case reports, where the penalty type was "insufficient technical and organizational measures to ensure information security". These GDPR penalty case reports, formally defining information security failures, accounted for the penalties issued to 81 different organizations.

B. Method

The method applied in the study was root cause analysis (RCA) to identify what caused the information security failures and what their impacts were. Root cause analysis as a method is a process which applies data collection, cause charting, root cause identification, and generation of recommendations. Only when root causes are determined can corrective measures that prevent future events of the type observed be specified [24].

The different RCA subtype methods can be summarized into the following three categories: a) chart type RCAs, which are constructed in the style of a flow chart, b) tabular type RCAs, which are constructed in a table with predefined column headings and categories and c) graphical RCAs, which visualize the results in a bar graph or any graphical display of numerical data [25]. The RCA method of this study is a mixture of tabular and graphical RCA types.

C. Set of criteria and the analysis

The criteria for this analysis were first the ISO/IEC 27001:2013 Annex A controls, which were initially used as root cause identifiers in each of 81 GDPR penalty cases [26]. Data was collected in a table which consisted of information about every GDPR penalty case and binary values corresponding to a specific information security failure, as exemplified in Table 1.

TABLE I. *GDPR PENALTY CASES AND INFORMATION SECURITY FAILURE BINARY VALUES*

	Penalty	**Failure a**	**Failure b**	**Failure c**
Case 1	10.000 €	0	1	1
Case 2	5000 €	1	1	1
Case 3	100.000 €	1	0	1
Case 4	8000 €	1	0	0
Case 5	600.000 €	1	0	0
Total	**723.000 €**	**4**	**2**	**3**

When this study was conducted, a new version of ISO/IEC 27001:2022 was published in Q4 2022 and the results were migrated to match the new version of the standard. As a result, 32 individual information security failures were identified, which included five failures that

could not be matched with any of ISO/IEC 27001:2022 controls.

These five failures were, however, included in the scope of the analysis because they were explicitly addressed by the supervisory authorities, and consequently were the cause of the issued penalties. In the presented results, these unmatched information security failures do not have the ISO number prefix, unlike the failures which were mapped to a specific ISO/IEC 27001:2022 control.

Penalty amount calculations for each information security failure were determined in the following way. The total penalty of a single GDPR penalty case was divided by the number of information security failures detected in the case. For example, in GDPR penalty case 1, illustrated in Table 1, with two detected information security failures and a total penalty of 10,000 euros, the cost of an individual failure was 5,000 euros. After that, the average was calculated for all information security failures, which became the penalty for each failure.

In the correlation analysis, p-values of the Pearson correlation were used, and outcomes where the p-value was lower than 0.05 were considered statistically significant. Information security failures which had a fairly strong (0.30 and above) correlation and statistical significance (p-value lower than 0.05), consisted of a total of 44 observations.

IV. Results

In this section, the results of the analysis are presented and discussed. ISO/IEC 27001:2022, ISO/IEC 27002:2022, and ISO/IEC 27701:2019 standards are used for interpreting the results.

A. The most frequent information security failures

The top 10 most frequent information security failures corresponding to ISO/IEC 27001:2022 controls are presented in Table 2.

TABLE II. *Top 10 most frequent information security failures corresponding to ISO/IEC 27001:2022 controls*

Control	Frequency	Penalty
8.3 Information access restriction	47	238,035 €
6.3 Information security awareness, education and training	32	40,604 €
5.12 Classification of information	31	623,332 €
5.14 Information transfer	18	10,182 €
8.24 Use of cryptography	18	335,304 €
8.15 Logging	14	331,892 €
8.29 Security testing in development and acceptance	14	1,146,388 €
5.10 Acceptable use of information and other associated assets	12	69,025 €
Human error	12	175,918 €
5.19 Information security in supplier relationships	9	343,139 €

The most common failure is the absence of "8.3 Information access restriction", where many cases showed that employees had unauthorized access to information that they should not have had. Another significant reason for data breaches is the insufficient "6.3 Information security awareness, education and training". Deficiencies in this control lead to a range of severe problems because employees are unaware of what is expected of them.

Another very critical failure is caused by insufficient implementation of "5.12 Classification of information", whereas information shall be classified based on organizational security needs and relevant interested party requirements, as well as PII [15] [17]. If this process is not carried out, relevant risk based controls cannot be applied, which leads to considerable compliance flaws [16].

The lack of control over "5.14 Information transfer" is a frequent failure. Unsecure and careless electronic messaging, including email, electronic data exchange, and social networking, often led to incidents. Another frequent failure is the unsuccessful implementation of "8.24 Use of cryptography". The type and strength of the cryptographic techniques required should be determined based on the classification of information [15].

A frequent failure is inadequate "8.15 Logging" because the lack of tracing user activities and access to PII in systems often led to data breaches. The absence of "8.29 Security testing in development and acceptance" was a cause of many failures. If proper security testing processes are not implemented during the system development life cycle, vulnerabilities are not discovered and fixed.

The lack of control over "5.10 Acceptable use of information and other associated assets" is a common cause of data breaches, followed by "Human error", which is not mapped to any specific ISO 27001 control. This failure, often resulting from insufficient information security awareness and training programs, can be further traced to poor organizational processes.

Finally, the absence of control over "5.19 Information security in supplier relationships", which is also a direct GDPR requirement [3], is a frequent cause among data breaches, underscoring the need for risk management related to the use of suppliers' products or services [15].

B. The most expensive information security failures

The top 10 most expensive information security failures corresponding to ISO/IEC 27001:2022 controls are presented in Table 3.

TABLE III. *Top 10 most expensive information security failures corresponding to ISO/IEC 27001:2022 controls*

Control	Penalty	Frequency
Technical data quality inconsistencies in systems leading to confidentiality breach	9,266,667 €	1
8.2 Privileged access rights	2,138,202 €	2
8.7 Protection against malware	1,214,167 €	2
8.29 Security testing in development and acceptance	1,146,388 €	14
8.32 Change management	765,217 €	3
5.12 Classification of information	623,332 €	31
5.24 Information security incident management planning and preparation	518,694 €	4
8.31 Separation of development, test, and production environments	510,303 €	4
8.5 Secure authentication	490,367 €	9
5.25 Assessment and decision on information security events	375,840 €	6

The most expensive failure relates to "Technical data integrity inconsistencies in systems leading to the confidentiality breach". Although this failure was not mapped to any specific ISO 27001 control, it can further be traced to controls that specify how information systems shall be developed and controls relating to "8.32 Change management", "5.12 Classification of information" and "8.29 Security testing in development and acceptance".

Further expensive failures result from inadequate "8.2 Privileged access rights". To prevent such incidents, the designation and use of privileged access rights should be restricted to ensure that only authorized users and service components are provided with privileged access [15]. More expensive failures resulted from the inadequacy of "8.5 Secure authentication", highlighting that a feasible authentication technique should be chosen to confirm the claimed identity of a user, software, messages, and other entities [15].

Expensive failures were also caused by the lack of control in "8.31 Separation of development, test, and production environments". In the absence of proper measures and procedures, developers and testers having access to production systems can introduce significant risks [15].

Expensive failures were caused by inadequacies in "8.7 Protection against malware", which should be based on malware detection, repair tools, and change management controls [15]. Many penalties were also caused by inadequacy in handling "5.24 Information security incident management planning and preparation", and further lack of implementation of control in "5.25 Assessment and decision on information security events".

C. *Information security failure correlations*

Table 4 presents the top three ISO/IEC 27001:2022 controls which have a positive correlation.

TABLE IV. TOP THREE POSITIVE FAILURE CORRELATIONS CORRESPONDING TO ISO/IEC 27001:2022 CONTROLS

Control 1	Control 2	Correlation	P-value
7.6 Working in secure areas	5.13 Labeling of information	1.00	***
5.26 Response to information security incidents	5.25 Assessment and decision on information security events	0.65	***
6.3 Information security awareness, education and training	5.10 Acceptable use of information and other associated assets	0.52	***
*$p < .05$, **$p < .01$, ***$p < .001$			

The controls "7.6 Working in secure areas" and "5.13 Labeling of information" have a very strong correlation. In the analyzed cases, there were many data confidentiality breaches, where employees had not handled information within the organizations' physical premises in a secure way. Often, paper documents or other physical media containing sensitive personal data were carried outside of secure areas and were later found in waste bins by complete outsiders.

This observation can also be seen in the correlation of controls "6.3 Information security awareness, education and training" and "5.10 Acceptable use of information and other associated assets". Therefore, the organization should ensure that employees are made aware of how information should be handled, especially when it comes to PII [17].

Controls "5.25 Assessment and decision on information security events" and "5.26 Response to information security incidents" are naturally correlated together. If incidents are not reported, further investigated, and fixed, then incidents remain unaddressed, which consequently causes data breaches to become larger and more severe.

V. DISCUSSION

As the regulatory requirements to comply with information security are becoming more demanding, intelligence is needed to support the decision-making to select the most effective controls to manage risks and threats. GDPR penalty cases are a fruitful and transparent ground to explore information security failures, their impacts, and respective solutions based on control frameworks.

This study presented a novel statistical model to analyze the root causes of information security in GDPR penalty case documents and match those root causes with ISO/IEC 27001:2022 annex A controls. Our work bridged the gap between regulation and information security by providing previously unpublished information about information security failures and respective controls how to prevent those failures.

A. *Conclusions*

Inadequate access restrictions and management of privileged access rights were very typical causes of data breaches. Deficiencies in information security awareness, education and training led to several contrasting issues, as staff members did not know what was expected of them. The lack of applying a proper information classification scheme was a cause of many different shortcomings because, without risk assessments, further risk-based controls such as proper cryptographic techniques, adequate logging, relevant measures against malware, or adequate change management and system security testing could not be implemented. Technical data quality inconsistencies in systems leading to confidentiality breaches were the cause of the biggest penalty imposed by the supervisory authorities.

The top correlation was between inadequate data-labeling schemes and employees' mishandling of sensitive information. Many data confidentiality breaches were caused by careless staff members carrying documents containing sensitive personal data outside the facilities of an organization, which were later discovered in waste bins by outsiders. Improper control in information security incident management led to data breaches being unaddressed, which furthermore caused failures to become more severe and larger, and therefore the incident management controls were naturally correlated.

B. *Limitations*

Our study is subject to three noteworthy limitations. Firstly, the quality of the GDPR penalty case reports authored by various supervisory authorities across EU member states may differ. Specifically, the 81 penalty case reports analyzed may not adhere to a uniform structure, and their precision and length may vary. Secondly, the data source of our study, the GDPR Enforcement Tracker, may not be entirely up-to-date. It is conceivable that additional GDPR penalty cases, beyond the 81 analyzed, were issued in the year 2020, but not yet included in the database at the time this study was conducted.

Thirdly, the penalty calculations of our study cannot be considered definitive. While we have analyzed 81 GDPR penalty cases, all of which can be classified under the penalty type "insufficient technical and organizational measures to ensure information security", 25 of these cases also referenced other GDPR articles, beyond the scope of information security requirements. It is important to note that supervisory authorities issue GDPR penalties holistically and do not differentiate penalty amounts to address a specific article when levying a GDPR penalty against an organization.

C. Further directions

From a practical perspective, organizations and auditors implementing ISO/IEC 27001:2022 may use our results to apply and verify controls based on their impact and interdependence. We encourage further research which would analyze GDPR penalty cases with the statistical methods we applied in our study with the ISO/IEC 27001, as well as with other similar standardization frameworks.

From a broader perspective, researchers and information security practitioners at other institutions are encouraged to use this study as a motivation to popularize the assessed and ranked information security controls in order to effectively manage the complex and challenging information security risks in organizations.

REFERENCES

[1] M. Gerber and R. von Solms, "Information security requirements – interpreting the legal aspects," Computers and Security, vol. 27, pp. 124–135, 2008

[2] M.T. Tayyaba Tariq, S. Ali, M.T. Safraz, M.S. De-La-Hoz-Franco, E. Butt, S.A. Starcangelo, D.V. Rad and V. Rad, "Combination of AHP and TOPSIS methods for the ranking of information security controls to overcome its obstructions under fuzzy environment," Journal of Intelligent & Fuzzy Systems, vol. 38, pp. 6075–6088, 2020

[3] 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, and repealing Directive 95/46/EC (General Data Protection Regulation)

[4] J. Ruohonen and K. Hjerppe, "The GDPR enforcement fines at a glance," Information Systems, vol. 106, p. 101876, 2022

[5] B. von Solms, "Information security – the fourth wave," Computers and Security, vol. 25, pp. 165–168, 2006

[6] A. Vaibhav, "Information security governance metrics: a survey and taxonomy", Information Security Journal: A Global Perspective, vol. 31, pp. 466–478, 2022

[7] M. Siponen and R. Willison, "Information security management standards: problems and solutions," Information & Management, vol. 46, pp. 267–270, 2009

[8] A. Calder and L. Gerard, ISO 27001 / ISO 27002 a Pocket Guide, 2nd ed., Cambridgeshire: IT Governance Ltd, 2013, pp. 12–14

[9] V. Diamantopoulou, A. Tsohou and M. Karyda, "From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls," Information and Computer Security, vol. 28, 645–662, 2020

[10] M.T. Dlamini and J.H.P. Eloff and M.M. Eloff, "Information security: the moving target," Computers & Security, vol. 28, pp. 189–198, 2019

[11] C. Garrison and C. Hamilton, "A comparative analysis of the EU GDPR to the US's breach notifications," Information & Communications Technology Law, vol. 28, pp. 99–114, 2019

[12] J. Wolff and N. Atallah, "Early GDPR penalties: analysis of implementation and fines through May 2020", Journal of Information Policy, vol. 11, pp. 63–103,2021

[13] S. Akhlaghpour, F. Hassandoust, F. Fatehi, A. Burton-Jones, and A. Hynd, "Learning from enforcement cases to manage GDPR risks", MIS Quarterly Executive, vol. 20, pp. 199–218, 2021

[14] W. Presthus and K.F. Sønslien, "An analysis of violations and sanctions following the GDPR," International Journal of Information Systems and Project Management, vol. pp. 38–53, 2021

[15] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

[16] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

[17] ISO/IEC 27701:2019 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)

[18] N.A. Chandra, R. Kalamullah, A.A.P. Ratna and T.S. Gunawan, "Information security risk assessment using situational awareness frameworks and application tools", Risks, vol. 10, pp. 165, 2022

[19] V. Monev, "Organisational information security maturity assessment based on ISO 27001 and ISO 27002", Proceedings of the 2020 IEEE International Conference on Information Technologies, 1-5, 2020

[20] B. Shojaie, H. Federrath and I. Saberi, "Evaluating the effectiveness of ISO 27001: 2013 based on annex A," Proceedings - 9th International Conference on Availability, Reliability and Security, 259-264, 2014

[21] H. Khajouei, M. Kazemi and S.H. Moosavirad, "Ranking information security controls by using fuzzy analytic hierarchy process," Information Systems and eBusiness Management, vol. 15, pp. 1–19, 2017

[22] M.I. Lopes, T. Guarda, and P. Oliveira, "Implementation of ISO 27001 standards as GDPR compliance facilitator", Journal of Information Systems Engineering and Management, vol. 4, 2019

[23] GDPR Enforcement Tracker, available at: https://www.enforcementtracker.com (accessed April-December 2021)

[24] J.J. Rooney, N. Lee and H. Vanden, "Root cause analysis for beginners," Quality Progress, vol. 37, pp. 45–53, 2004

[25] D. York, K. Jin, Q. Song, and H. Li, "Practical root cause analysis using cause mapping", Lecture Notes in Engineering and Computer Science, vol. 2, pp. 985–989, 2014

[26] Suorsa, M. and P. Helo, Information security failures identified and measured – ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis, Information Security Journal: A Global Perspective

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

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

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

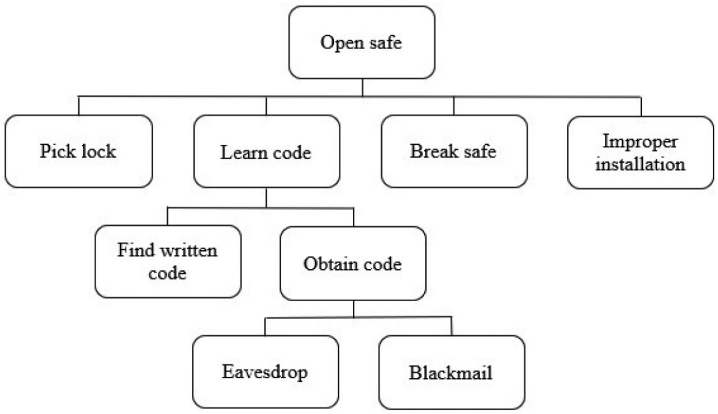

Figure 1. Example of attack tree.

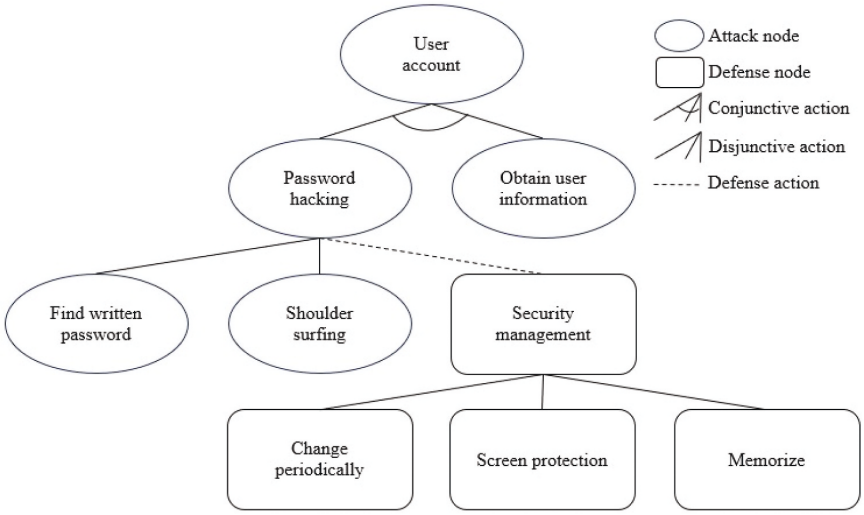

Figure 2. Example of attack-defense tree.

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.

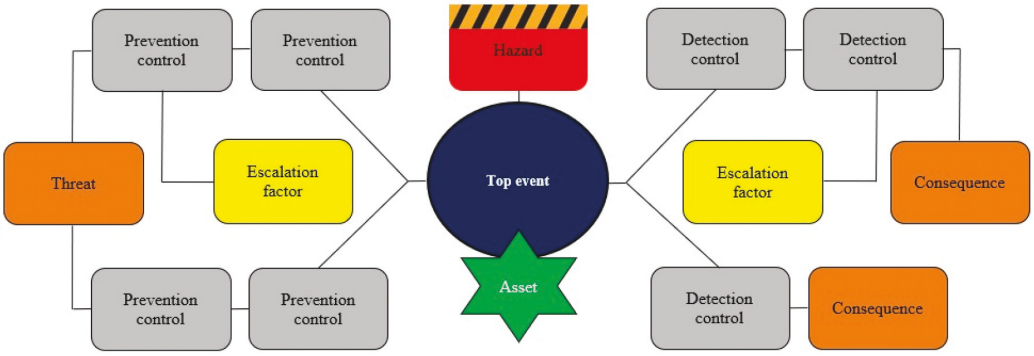

Figure 3. Elements of the bow-tie method.

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

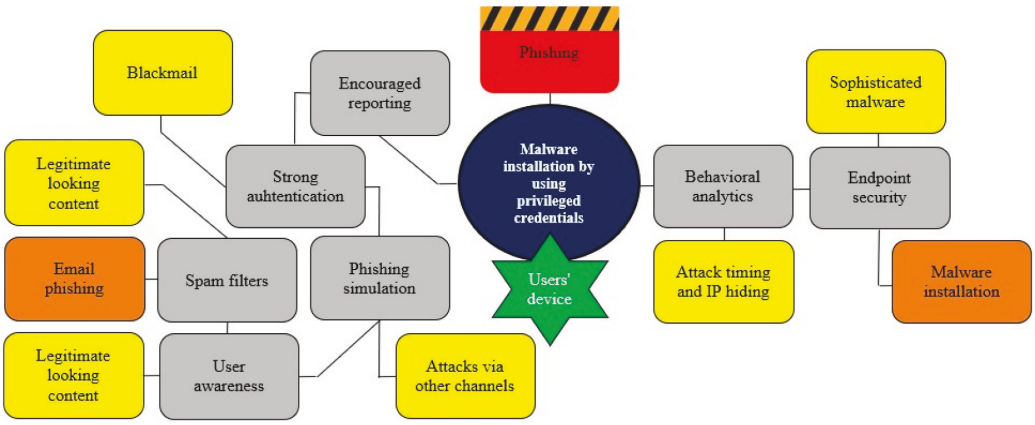

Figure 4. Phishing attack example visualized using a bowtie model.

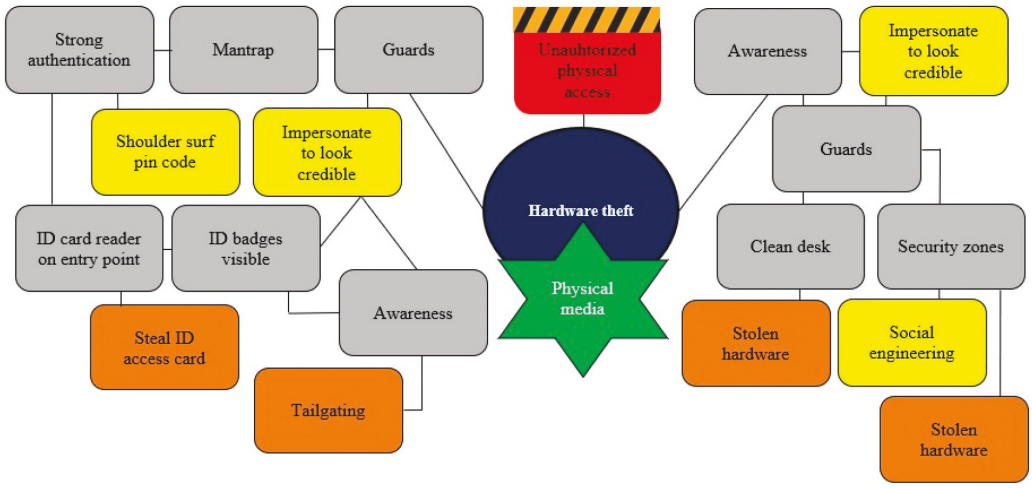

Figure 5. Unauthorized entry attack example visualized by bowtie model.

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