Information Security Journal: A Global Perspective

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

Key drivers of information security culture: A survey and exploratory factor analysis in an energy retail organization

M. Suorsa , P. Helo & J. Petman

To cite this article: M. Suorsa , P. Helo & J. Petman (01 Jul 2026): Key drivers of information security culture: A survey and exploratory factor analysis in an energy retail organization, Information Security Journal: A Global Perspective, DOI: 10.1080/19393555.2026.2690536

To link to this article: https://doi.org/10.1080/19393555.2026.2690536

Published online: 01 Jul 2026.

INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE
https://doi.org/10.1080/19393555.2026.2690536

Key drivers of information security culture: A survey and exploratory factor analysis in an energy retail organization

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

[a]School of Technology and Innovations, University of Vaasa, Vaasa, Finland; [b]Department of Mathematics and Statistics, University of Jyväskylä, Jyväskylä, Finland

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 (Löschel et al., 2010; Yusta et al., 2011). 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 et al., 2025). Other notable examples include Australia's Security of

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

Critical Infrastructure Act (Lloyd-Jones, 2025), Singapore's Cybersecurity Act (Gorian, 2020), and Japan's Cybersecurity Management Guidelines for Critical Infrastructure (Mochinaga, 2024).

Cybersecurity culture within the energy sector shapes organizational practices and employee behavior aimed at protecting critical assets, data, and information, thereby enhancing resilience and establishing security as a strategic priority (AlHogail & Mirza, 2014). 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 (AlHogail & Mirza, 2014; Gcaza & von Solms, 2017).

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 catalog 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). 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

Table 1. Survey questions.

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	Behavior	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	Behavior	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	Behavior	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	Behavior	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	Behavior	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	Behavior	Access and trust

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 toward users' behavioral aspects (Mahfuth et al., 2017; Tang et al., 2016), 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 (Sanskriti & Astitwa, 2018; Siponen & Willison, 2009). 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 mind-set 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).

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 (Hu et al., 2012; Vincent et al., 2018). 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 (da Veiga & Martins, 2014).

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.

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

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

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.

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

2.4. Exploratory factor analysis

Exploratory factor analysis (EFA) is a statistical technique used to identify underlying patterns in data without predefined assumptions. EFA

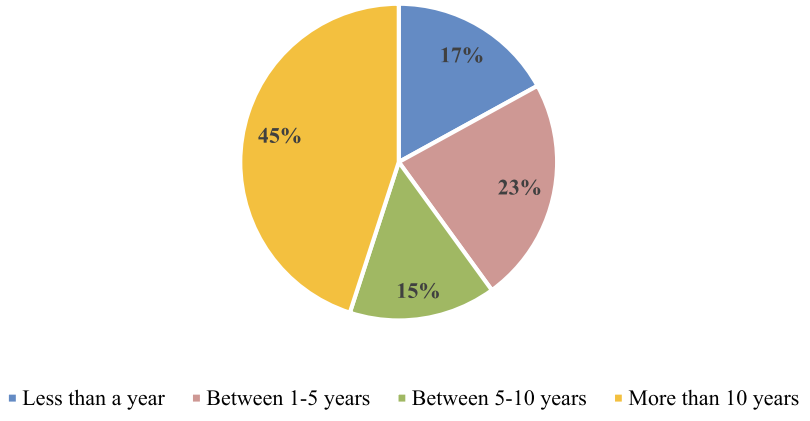

Figure 1. Length of employment of survey respondents.

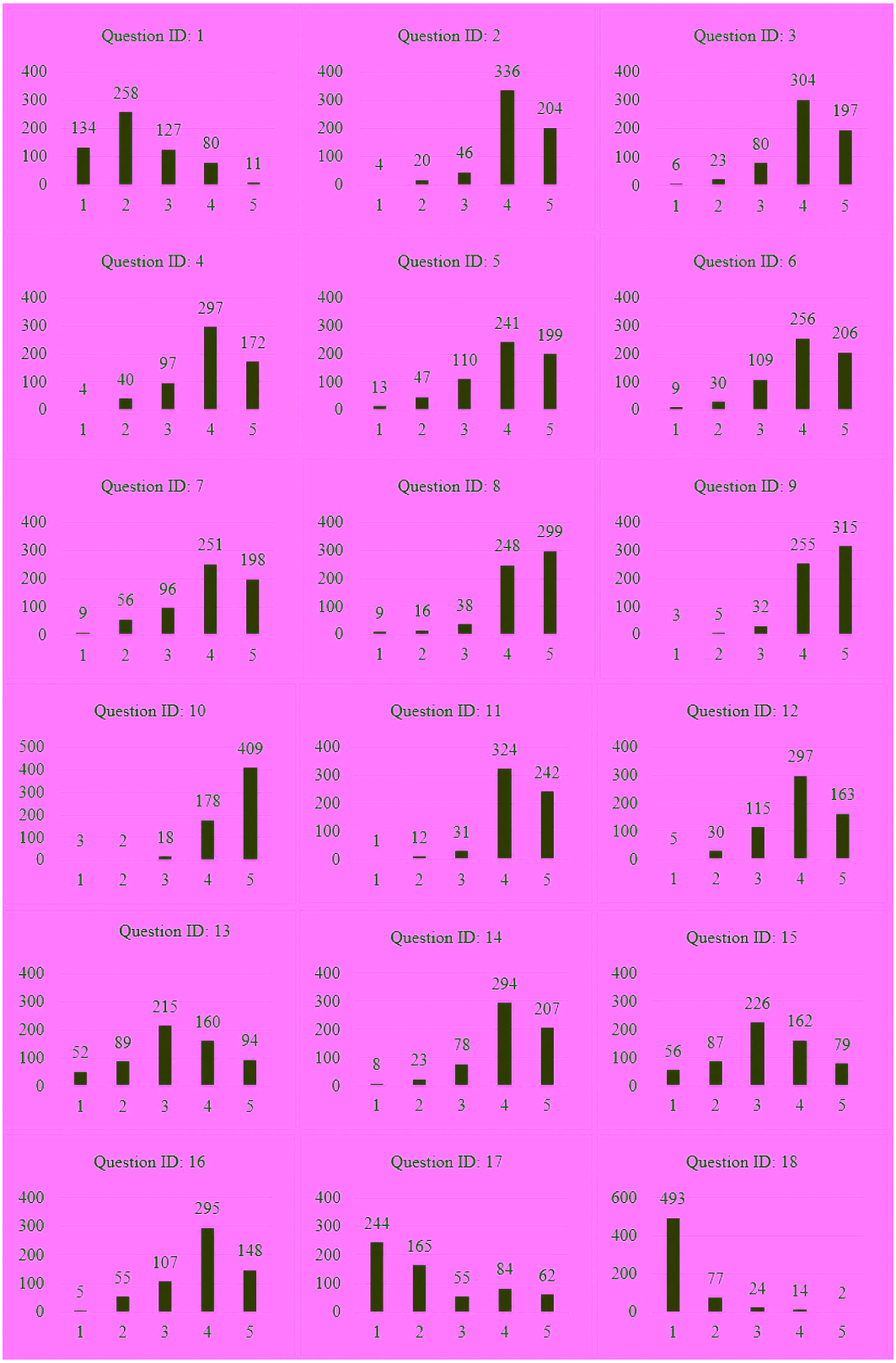

Figure 2. Histograms of survey questions.

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 ($p < .001$), 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 ($p < .001$). 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.

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

Table 3. Survey questions, culture domains, and loadings.

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

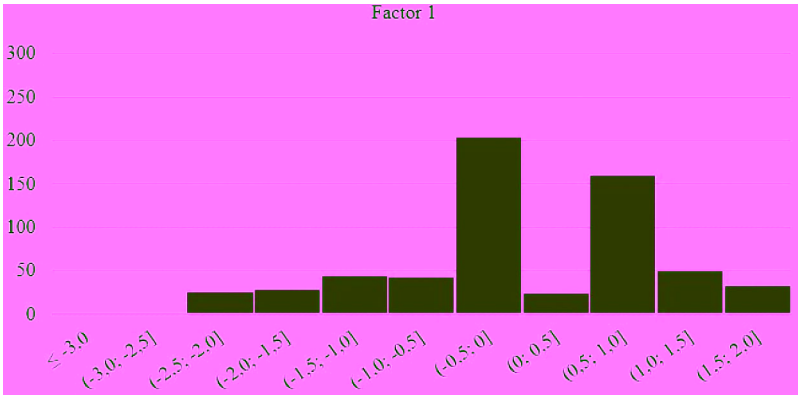

Figure 3. Factor score distribution for factor 1.

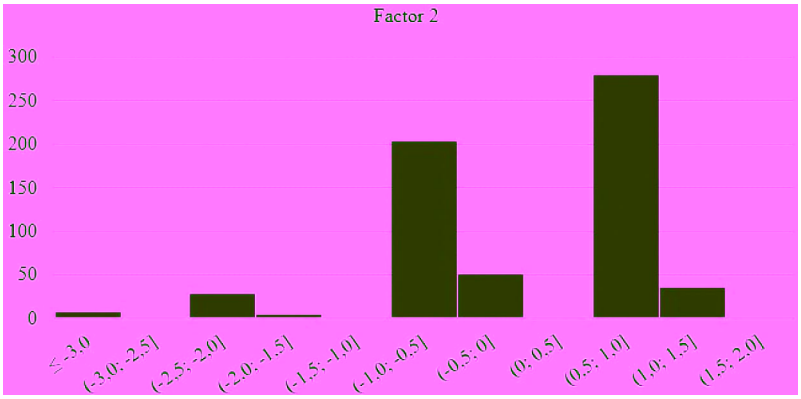

Figure 4. Factor score distribution for factor 2.

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, Figure 4, and Figure 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

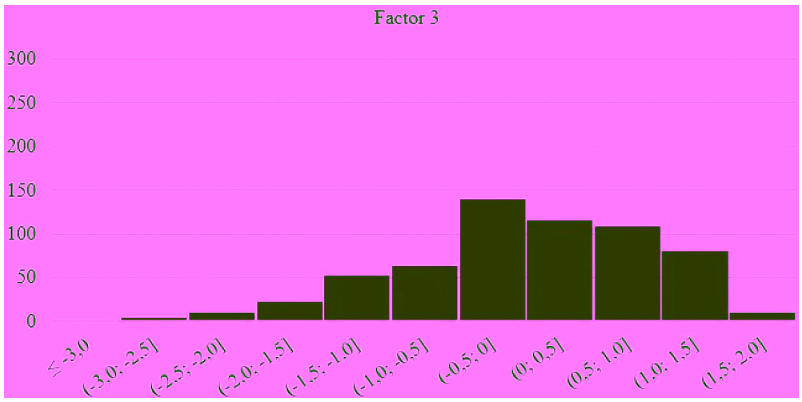

Figure 5. Factor score distribution for factor 3.

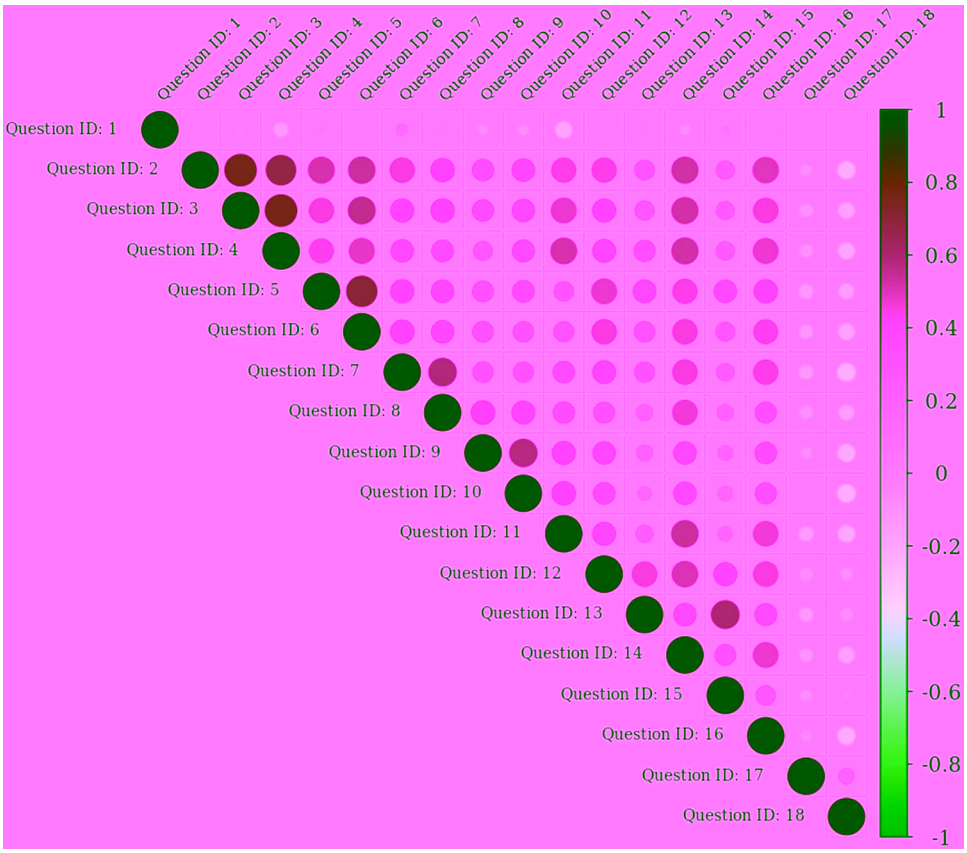

Figure 6. Correlation plot of the original survey variables.

individual responses relate to the underlying latent constructs identified in the analysis.

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 7 displays a similar correlation plot, illustrating the relationships between the original

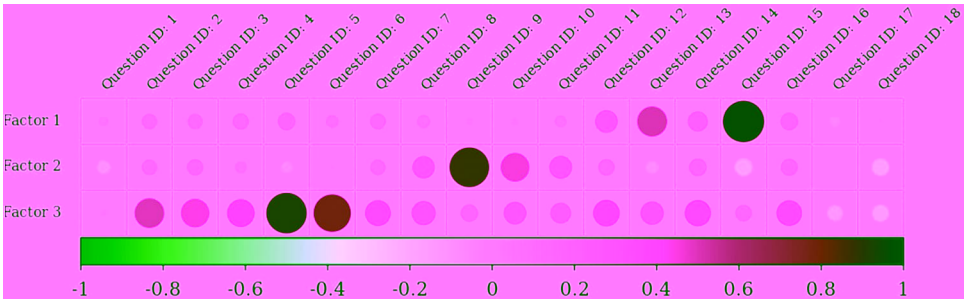

Figure 7. Correlation plot between original survey variables and factor scores.

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

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	Behavior	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	Behavior	Access and trust

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.

The statistical analyses were conducted using the R programming language. EFA was performed using the R packages *psych*, *EFAtools*, and *EFA.dimensions*, which were employed for factor extraction, assessment of factorability, and determination of the number of factors. Graphs were generated using functions available in R and the applied analysis packages.

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 acknowledgment and rewarding of positive security practices, motivating employees to actively contribute to secure behaviors and embrace a proactive culture of information security risk mitigation.

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 (Folorunso et al., 2024; Putri 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 acknowledgment 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.

Author contributions

CRediT: **M. Suorsa:** Conceptualization, Investigation, Methodology, Project administration, Validation, Visualization, Writing – original draft, Writing – review & editing; **P. Helo:** Supervision; **J. Petman:** Data curation, Formal analysis.

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
J. Petman http://orcid.org/0009-0002-6394-9777

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*, *33*(2), 242–266. https://doi.org/10.1108/ICS-11-2023-0214

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

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

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

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

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

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

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

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

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. *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

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, J. C., III, 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), 255. https://doi.org/10.69554/JHEV8231

Folorunso, A., Mohammed, V., Wada, I., & Samuel, B. (2024). The impact of ISO security standards on enhancing cyber-security 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. (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

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

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 & 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)* (pp. 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*(6), 1251–1263. 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

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*(3), 247–262. https://doi.org/10.1023/A:1010787607771

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

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. *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

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476–486. https://doi.org/10.1016/j.cose.2009.10.005

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*(3), 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