International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Human Factor Vulnerabilities in Energy Industry Cybersecurity: Assessing Employee Awareness and Behavior in Breach Prevention

Benjamin Panful[1], Barnabas Apaflo[2], Abimbola Filani[3], Kenneth Nnadi[4], Nasiru Hutchful[5]

[1]Lake Land College, USA
[2]Texas A&M University
[3]Department of Business Information Systems, Central Michigan University, Michigan, USA
[4]University of Oregon, USA
[5]Department of Computer Science and Engineering, University of Mines and Technology, Ghana

ABSTRACT
Cyberattacks are a prime focus on the energy sector, and employees are typically identified as the weakest link. This is a systematic literature review (SLR) that has identified 103 studies, using "("cybersecurity" OR "information security") AND ("energy industry" OR "power sector" OR "oil and gas" OR "utilities" OR "critical infrastructure") AND ("human factor" OR "employee behavior" OR "awareness" OR "insider threat" OR "phishing" OR "social engineering")" as search keywords across academic databases, 40 of which are included in the further analysis and synthesis in accordance with PRISMA guidelines. The review lists six common human factor vulnerabilities, including: awareness and training vulnerabilities, insider vulnerabilities and negligence, social engineering and phishing, compliance vulnerabilities and policy compliance, organizational culture, and ICS/SCADA-specific vulnerabilities. Results confirm that although technical precautions are essential, human actions, lack of compliance, and insufficient knowledge are most often exploited during breaches. Cultural and motivational factors also strongly influence security outcomes. The analysis identifies the gaps on long term training effectiveness, the realization of the security culture that was carried out to date, and the incorporation of human-based actions to technical systems. The review summarizes the scattered knowledge and offers a systematic approach to managing the risks posed by employees in cybersecurity of energy industries.

Keywords: Insider threats, social engineering, compliance behavior, industrial control systems (ICS), SCADA security

1. INTRODUCTION

Cybersecurity has emerged as another issue that cannot be avoided in the energy sector as more critical infrastructures are being digitized in terms of their operation, monitoring, and control. According to Krause et al. (2021), the digitalization of the power infrastructure has increased the scale of the communication infrastructure and has provided a greater attack surface to malicious actors, with blackouts already caused by cyber incidents in several countries. Likewise, research demonstrates that energy is one of the five most

targeted industries globally, and spear phishing, insider abuse, and state-sponsored attacks that take advantage of vulnerabilities in organizations are among the top (Wueest, 2014).

As important as technical protection is, literature continues to agree that the human factor is the weakest point of cybersecurity in the energy industry. Some studies emphasize the fact that employees are not just spectators but, in most cases, they are the same points of entry where the breach takes place, either accidentally or due to ignorance or deliberate acts of insiders (Ghafir et al., 2018). Various surveys of SCADA and industrial control system (ICS) events confirm that incidents of operator errors, lack of good compliance, and insufficient training were pivotal factors that led to failures in the systems (Nazir et al., 2017; Alcaraz and Zeadally, 2015).

The use of training and awareness programs is very common, but the problem is that these programs do not always result in a lasting change in behavior. As Kirlappos and Sasse (2011) indicate, phishing education is often not effective since workers learn to cheat in the test without necessarily adopting safe habits. Likewise, studies on the topic of awareness campaigns indicate that even after several investments, organizations cannot embed secure habits, and campaigns fail due to their application of compliance-based, instead of motivation-based approaches (Bada et al., 2019). This is reminiscent of the more general literature on compliance psychology that postulates that the key motivation forces to encourage employees to comply with security policies are protection motivation and deterrence (Herath and Rao, 2009).

Energy sector is a special industry since the infrastructure in the industry follows highly complex cyberspace conditions. The review of oil and gas industry cyber-attack examples suggests that cyber-attack patterns may be replicable, and human operators are tempted to assist in gaining access, either in spear phishing campaigns, or social engineered attacks (Stergiopoulos et al., 2020). Furthermore, the use of renewable energy systems also creates additional points of vulnerability. Ekechukwu and Simpa (2024) argue that the sustainability of such an investment in renewable energy relies on employee awareness and safety, as the safety of renewable energy systems may be jeopardized by cyber threats, which may undermine the reliability, efficiency and safety of these systems.

Although there is a growing amount of research on technical defenses, the extent to which employee awareness, organizational culture, and vulnerabilities to behavioral aspects combine to open up the energy sector to cyber threats has not been adequately synthesized. Other literature recognizes the problem but addresses it in general security contexts, with an incomplete picture of the particular human factor problems. For instance, Nazir et al. (2017) highlight gaps in SCADA operator training, while recent frameworks on cybersecurity culture stress organizational responsibility for awareness building (Georgiadou et al., 2022). Nevertheless, none of the reviews have brought together these understandings in sectors and types of attacks to offer a humanistic evaluation of energy infrastructure.

The study fills that gap by performing a systematic literature review (SLR) to identify, analyze, and synthesize evidence of human factor vulnerabilities in cybersecurity in the energy industry. Raising awareness of employees, training performance, and weaknesses in behavior, including vulnerability to social engineering, this review aims to explain the level of knowledge, identify the recurring vulnerabilities, and determine the efficacy of the organizational interventions. The contribution of the paper is that it helps to bring together fragmented evidence, compare the existing frameworks, and suggest a conceptual framework of the approach to employee-based risks in the energy sector.

In order to organize this systematic literature review, the following research questions were developed:

RQ1: What are human factor weaknesses identified in cybersecurity of the energy industry?

RQ2: How is awareness of employees, training, and compliance related to cybersecurity resilience in energy infrastructures?
RQ3: How does an organizational culture and motivational factor contribute to the behavior of secure or insecure employees?
RQ4: What are some of the comparisons between human factor vulnerabilities in the energy sector and other critical infrastructures including water, ICT, and Industry 4.0?
RQ5: Which gaps are there in the current strategies to combat human factor vulnerabilities, and where is future research headed?
The questions aided in structuring the systematic screening, synthesis, and analysis of the selected studies and enabled the review to provide a comprehensive picture of the weaknesses of employees, and the impact of those on the security of the energy industry.
The comparative analysis shows that definitions of cybersecurity vary in many settings; the authors suppose that a representative definition should be adopted, which incorporates confidentiality, integrity, availability and resilience and corresponds to the organizational risk priorities (Schatz et al., 2017). Having this in place, numerous studies have been conducted on confidentiality, integrity, availability and resilience within different energy sectors that constitute cybersecurity within the sectors.

1.1.Cybersecurity in Critical Energy Infrastructures

The susceptibility of critical infrastructures, especially in the energy sector, is not a novel issue that has only been reported within a decade. The industry report published by Symantec highlighted that the energy sector is currently ranked as one of the five most targeted sectors globally, and the attackers are taking advantage of external technical vulnerabilities as well as internal employee vulnerabilities (Wueest, 2014). The history of ICS cyber-attacks, including the Stuxnet and the Ukrainian power grid outages, shows how the attacks were used to target human-machine interfaces, failures in decision-making by the operators, and unsecured access points (Hemsley and Fisher, 2018). Attack-defense modeling (e.g., defense trees) can be used to economically assess security investments in CI and is consistent with risk-based systems security engineering of interdependent infrastructures (Ten et al., 2010).
Critical infrastructure protection reviews point out the duality of the threat: technical vulnerability and human fallibility. Alcaraz and Zeadally (2015) state that situational awareness and operator reliability are essential to the resilience of industrial systems, in addition to perimeter protection. Similarly, Nazir et al., (2017) determined that the lack of training and human-oriented controls in the SCADA setting compounded the effects of attacks.

1.2.The Human Factor in Cybersecurity

Many publications come to the same conclusion that employees are still the weakest link in energy cybersecurity. Ghafir et al. (2018) define human factors as the actual points of entry, where breaches happen, and list negligence, lack of awareness, and malicious insiders as common threats. Through a systematic study of a worker's behavior, phishing, failure to obey security rules and vulnerability to social engineering will always fail to make any organizational security (Pujari and Hussain, 2024).
This is also backed by behavioral studies in information security. As Kirlappos and Sasse (2011) show, security training does not always lead to long-term behavior change since it is compliance-based and not motivation-based. This is reflected in the awareness campaign discussion, in which it is stated that when the organizational strategies that do not keep the employees busy are reused, the organization utilizes the same strategies (Bada et al., 2019).

1.3.Awareness, Culture, and Compliance

The creation of a culture of cybersecurity awareness has become one of the primary themes of literature. Georgiades et al., (2022) believe that the tendency of employees to internalize security practices is highly dependent on the organizational culture. The theory of protection motivation has been used to describe compliance behavior with the idea that deterrence and personal risk perception are important predictors of secure behavior (Herath and Rao, 2009). On the same note, MISQ research on information security policy compliance notes that rationality-based beliefs by employees determine compliance with rules (Bulgurcu et al., 2010).

This is further supported by evidence in the oil and gas sector. There have been reports of repetitive vulnerability after poor training of the working force and absence of systematic awareness systems (Pothana et al., 2024). It has been mentioned on many occasions that one of the most hazardous risks in a critical infrastructure environment is insider misuse, and that special awareness programs that reflect the realities of the operational environment are required (Olubudo, 2024).

1.4.Social Engineering and Insider Threats

Social engineering is consistently cited as the most common human vector of attack in the energy industry. Klimberg-Witjes and Wentland (2021) discuss the way that employees are constructed as "deficient users" in organizational narratives and blamed for breaches, while systemic factors are ignored. Phishing and spear-phishing continue to be the most common enablers of targeted attacks against energy firms (Wueest, 2014). Direct research into employee susceptibility has validated that even after several campaigns, a significant proportion of staff remain vulnerable to simulated phishing attacks (Kirlappos and Sasse 2011).

Insider threats are another layer of human vulnerability. Nazir et al. (2017) have documented that operator error and negligence in the SCADA operations have led to cascading failures. A survey of oil and gas cyberattacks suggests that insiders (intentional and unintentional) were connected to most high-profile incidents (Stergiopoulos, 2020). These findings outline the need for more complete approaches to malevolence and accidental carelessness.

1.5.Evolving Threat Landscape in Energy Systems

As distributed and renewable technologies are being taken up by the energy industry, the complexity of cyber risks increases. Krause et al. (2021) note that digitization and renewable integration increase the attack surface and that there is a need for policies, procedures, and awareness to accompany technical defenses. According to studies on renewable energy systems, cybersecurity is a precondition for sustainability because the reliability, efficiency, and safety of renewable investments can be compromised by cyber threats (Ekechukwu & Simpa, 2024).

Our cross-sector scan shows that digital transformation, legacy assets, and human error are contributing to increasing exposures. Phishing, ransomware and insider abuse are the most common threats; and mitigation options include structured risk assessment, incident response and employee training (Asimiyu, 2024).

Advanced Persistent Threats (APTs) are also an important player. Yusof (2024) calls them longer-term and stealthy campaigns that are more likely to involve social engineering, manipulation of insiders, and zero-day attacks on critical infrastructures. Defensive analysis of oil and gas-related attacks has proven that even the most sophisticated campaigns (as per the sources) continue to use phishing and stealing credentials as a first step before expanding their attacks (Pothana, 2024).

1.6.Comparative Insights from Other Sectors

Although the focus of this review is on the energy industry, several cognate domains offer instructive com-

parative lessons about human factor vulnerabilities.

Water Sector:

Analysis of cybersecurity incidents in the water sector shows that human error and lack of awareness are just as important as in the energy sector. A systematic review of water network failures attributed the cause of large-scale failures to operator misconfiguration, poor incident response and lack of awareness programs (Hassanzadeh et al., 2020). The parallels with energy SCADA systems suggest that there is a lot of cross-sector learning to be done, especially in areas of staff training and system robustness.

ICT and General Critical Infrastructure:

More general studies of ICT-related attacks in critical infrastructures identify insider attacks and employee negligence as key issues. Nazir et al., (2017) pointed out that the most common weakness across critical infrastructures is the lack of systematic operator awareness training. Alcaraz & Zeadally (2015) go on to suggest that critical infrastructure security must be considered a socio-technical problem, in which technology can't make up for the lack of employee awareness. These studies indicate that the human factor remains a cross-cutting vulnerability regardless of which infrastructure domain is in question.

Industry 4.0 and Digitalization:

Industry 4.0 and the digitalization of the industrial world continue to present both opportunities and threats to cybersecurity. Analysis of Cybersecurity risks for Industry 4.0 shows that digitized systems are expanding the attack surface and the employees are not really aware of how to manage complex digital ecosystems (Alqudhaibi et al., 2022). Similarly, risk management research indicates that highly digitized industrial environments are particularly susceptible to human decision-making errors compounded by cognitive overload (Tupa et al., 2017). These results are consistent with the challenges that the energy sector is facing where grid digitalization and renewable integration are creating new risks that must be balanced by employee readiness and organizational culture.

Organizational Behavior and Psychology:

Information from behavioral science and organizational psychology is also a factor in understanding vulnerabilities. The Theory of Planned Behavior (TPB) is commonly referenced as a reason why employees do not adhere to cybersecurity policies, as attitudes, perceived norms, and perceived control are key predictors of secure behavior (Ajzen, 1991). The theoretical basis is supported by empirical data in energy which confirms that behavior cannot be assumed as a given without the inclusion of psychological and cultural variables.

Ransomware and Emerging Threats:

Finally, the recent attacks on critical infrastructure in a number of industries illustrate how attackers use human factors as entry points. According to reports, phishing emails, poor password habits and employee negligence are the most popular ransomware attack enablers (Mohammed, 2019). This always makes for a powerful combination, and even as technical defenses are getting more sophisticated, the fact that attackers are still playing on human weaknesses confirms the universal importance of awareness and behavioral defenses.

2. METHODOLOGY

This study is based on a systematic literature review (SLR) method, which was organized in line with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. The goal was to find, filter, and synthesize research about human factors vulnerabilities in energy industry cybersecurity, particularly employee awareness and behavior in the context of preventing breaches.

2.1.Identification

A total of 103 research papers were identified by the authors as potentially relevant to the topic. These articles were peer-reviewed journal articles, conference proceedings, industry reports, and doctoral theses, covering the period from some of the earliest foundational works on critical infrastructure protection to recent analyses of human-centric vulnerabilities in the energy sector. The scope covered both studies directly related to the energy industry as well as contextual studies related to other critical infrastructures (e.g., water, Industry 4.0) or human factors in cybersecurity in general.

2.2.Screening

All 103 papers were systematically reviewed. Screening was conducted in three stages:

The first is the title and abstract screening. Papers that had no relevance to cybersecurity, human factors, or critical infrastructures were initially excluded.

The second was the full-text review. The second stage consists of detailed reading of the documents to determine their relevance to the focus on human factor vulnerability in the energy sector.

Finally, the eligibility check uses inclusion and exclusion criteria for consistency.

2.3.Eligibility Criteria

The following inclusion and exclusion criteria were used:

Inclusion Criteria:

Started with special studies on cybersecurity in the energy sector (electricity, oil, gas, renewables). Then papers that address human factors including employee awareness, behavior, social engineering, insider threats, compliance or organizational culture. Also included empirical studies, systematic reviews, theoretical models and case studies relating to human vulnerabilities. Comparable research in relevant critical infrastructures (water, ICT, Industry 4.0) where lessons can be transferred

Exclusion Criteria:

Technical white papers with no mention of employees, awareness, or human vulnerabilities, works that are not located in the energy or closely related critical infrastructure sectors and redundant or duplicate studies with overlapping content.

2.4.Categorization

At the end of screening, the papers were classified as follows:

Eligible for Final Review Directly related to human factor vulnerabilities in energy sector cybersecurity. These papers were the main evidence base for the synthesis.

Not included: (not suitable for inclusion because of their purely technical focus, lack of sectoral relevance, or inadequate treatment of employee awareness) Exclusion was justified in writing (e.g. technical focus, excluded energy scope).

Background/Contextual: Were used to provide relevant contextual information (e.g., frameworks, comparative perspectives, historical grounding) but were not included in the final synthesis. Background and discussion sections were supplemented with material from these papers.

The table below shows the summary of the inclusion and exclusion criteria

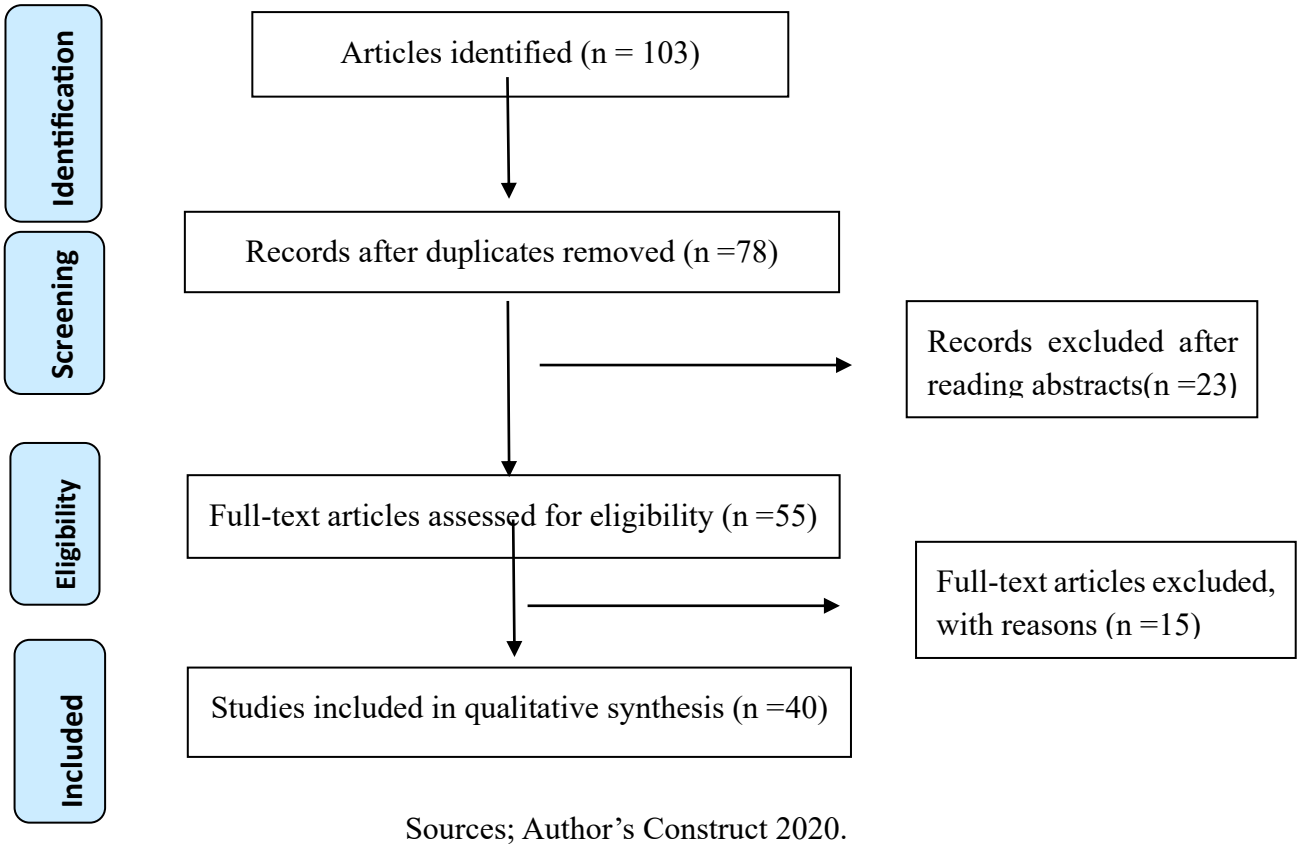
Table 1: Summary of inclusion and exclusion criteria

Criterion	Included	Excluded
Sector Focus	Energy industry (electricity, oil, gas, renewables) or	Non-energy areas outside the scope of critical infrastructures

	closely related CI (e.g., SCADA, ICS).	
Human Factor Relevance	Handles employee awareness, training, behavior, compliance, social engineering, insider, or organizational culture.	Studies that are purely technical and have no human/organizational dimension.
Study Type	Empirical studies, case studies, systematic reviews, theoretical frameworks, industry/government reports	Editorials, non-scientific commentaries, copies
Time Period	No limit, if the study will provide useful information on energy cybersecurity human factors.	Outdated work that is not directly relevant

2.5.Prisma Flow of Screening and Selection

Figure 1: PRISMA Flow diagram showing the article selection process in the study.



Sources; Author's Construct 2020.

3. RESULTS

Synthesis of 40 eligible studies identified six human factor vulnerabilities in energy industry cybersecurity: (1) awareness and training, (2) insider threats and employee negligence, (3) social

engineering and phishing vulnerabilities, (4) compliance and policy adherence, (5) organizational culture and security environment, and (6) ICS/SCADA-specific human vulnerabilities.

3.1.Awareness and Training Gaps

While the promise of AI/ML is earlier anomaly detection and faster response to APTs, adaptive human adversaries can poison data and launch AI-powered phishing, highlighting the need for human oversight in conjunction with automation (Manoharan & Sarker, 2023).

Several studies have shown that awareness programs alone are not enough to bring about long-term behavioral change. Kirlappos & Sasse (2011) noted that security training against phishing is often ineffective because employees are trained to run only to satisfy compliance audits rather than internalize secure behavior. Similarly, a study of cybersecurity awareness campaigns found that most campaigns are ineffective at changing behavior because they are based on fear appeals and compliance-based models rather than motivational models (Bada et al., 2019).

Behavioral science offers other explanations. One study claimed that people are governed by cognitive biases and heuristics that make awareness campaigns less effective unless training is linked to intrinsic motivation (Pfleeger & Caputo, 2012). A similar empirical study in the oil and gas industry also found recurrent training gaps that exposed workers to manipulation in their working environment (Pothana, 2024). Together, these results indicate that although training is commonly used, it is not often designed to create sustained changes in employee decision-making (Pouraimis et al., 2019).

3.2.Insider Threats and Employee Negligence

The insider threat is one of the most enduring vulnerabilities in the literature reviewed. Nazir, et al (2017) had reported that human error by operators is the most common reason for system failures in SCADA environments. Surveys of cyberattacks in the oil and gas industry have indicated that both malicious insiders and careless employees played a key role in many incidents (Stergiopoulos, 2020).

A further study of the US electric sector pointed to the direct correlation between employee training and awareness gaps and greater exposure to insider threat (Glenn et al., 2016). These results confirm that insider threats are not only a technical security issue but are closely linked with human awareness, motivation, and compliance with security processes.

In addition to malicious insiders, employee carelessness continues to be a common weakness in the energy industry. Recent studies have indicated that human error is involved in most cyber-attacks, especially where staff do not abide by access control or basic security practices, and systems remain unprotected even with the most advanced technical controls (Ajayi et al., 2025). Another example of how lack of diligence is misused is in the attacks against Ukraine's power grid, where lack of process discipline and training are undermining phishing campaigns to gain access to operator accounts and disrupt power supply (Clemente 2018).

3.3.Social Engineering and Phishing Vulnerabilities

Social engineering, and in particular phishing, was found to be the most common attack vector to exploit human vulnerabilities. The Symantec report highlighted that many of the most damaging breaches in the energy sector were caused by spear phishing campaigns and that operators of critical infrastructure, energy utility companies in particular, need to be aware of these risks and prepare for them (Wueest, 2014).

Klimburg-Witjes & Wentland (2021) critically reviewed the tendency for organizational narratives to position employees as poor users, thus masking systemic problems, whilst also recognizing that phishing success rates are still overwhelmingly high. Nazir et al., (2017) further confirmed that operator susceptibility to phishing directly exposed SCADA environments to intrusions. These results demonstrate

that, despite a decade of awareness campaigns, phishing remains an effective attack vector that exploits fundamental human trust and decision-making biases.

The number of attacks on CI is growing and becoming more sophisticated, and digital intrusion can result in physical damage in certain industries, such as power and transport (Lehto, 2022). Social engineering attacks continue to be one of the most pervasive human-factor threats, and phishing, pretexting, baiting, and tailgating are often mentioned as ways to exploit psychological triggers such as trust, fear, urgency, and curiosity. Oluremi et al. (2025) address the mechanisms of getting around technical barriers directly by targeting individuals as employees, with a focus on the need for awareness and training to reduce vulnerability.

3.4.Compliance and Policy Adherence

Compliance research highlights the role of employees' attitudes and perceptions in determining whether or not policies are actually followed in practice. Herath & Rao (2009) applied protection motivation and deterrence theory and showed that compliance is a non-automatic process that relies on risk perception and perceived control.

This is also supported by the MISQ studies which indicate that rationality-based beliefs and attitudes to the organization are significant determinants of rule adherence (Bulgurcu, 2010). Empirical research has shown that unless employees perceive both personal responsibility and organizational support, average compliance rates with security policies are low (Puhakainen & Siponen, 2010). These results suggest that compliance is not just a question of awareness, but requires a change in organizational culture, motivation and individual attitudes.

3.5.Organizational Culture and Security Environment

A recurring theme is the role of organizational culture in employee behavior. Georgiadou et al. (2022) suggested a Cybersecurity Culture Framework, in which the integration of awareness into the organizational environment is a precondition for achieving sustainable security. Parsons et al., (2010) also highlighted the strong mediating effect of cultural and environmental factors on employee security behavior, pointing out that security is not an individual choice but rather one embedded within the norms of the organization.

This is also confirmed by comparative sectoral analysis. Ekechukwu & Simpa (2024) also noted that a secure operational culture is linked to the viability of investment in renewable energy systems since "cyber risks can jeopardize the reliability, efficiency, and safety of renewable projects." Organizational security culture has often been neglected in this scope. Together, these studies suggest that developing an organization-wide security culture is just as important as individual awareness training in reducing vulnerabilities.

The study highlights that the EU NIS2 directive cannot be met by technical safeguards alone, but needs a strong cybersecurity culture across the critical infrastructures. Kioskli et al. propose that organizational resilience depends on the internalization of security values and behaviors in everyday operations and conceptualize culture as a strategic pillar together with technology and regulation.

3.6.ICS/SCADA-Specific Human Vulnerabilities

The literature has shown repeatedly that ICS and SCADA systems are uniquely susceptible to human errors due to their complex socio-technical environments. Nazir et al., (2017) reviewed SCADA security methods and concluded that operator negligence, lack of situational awareness, and lack of training contributed significantly to SCADA vulnerability. This is supported by historical surveys of ICS incidents,

which have indicated that human factors contributed to cascading system failures in incidents ranging from Stuxnet to the Ukraine blackouts (Hemsley, & Fisher, 2018).

Other evidence is from smart grid and distributed energy environments. Krause et al. (2021) warned that the digitalization of power grids increased the attack surface and, therefore, technical controls were necessary, but not sufficient, without awareness and training of operators. Yusof (2024) also illustrated how APTs are using both technical vulnerabilities and social engineering techniques to gain persistent access to energy systems. Smart grids are more concerned with availability and real-time performance than with heavy cryptography, making it more difficult to defend against attacks on resource-constrained field devices; suggested mitigations include deep packet inspection, proper encryption, and increased physical security (Line et al., 2011).

In the case of oil & gas, IT/OT convergence and IIoT growth expand the attack surface, exposing downstream-to-upstream operations to malware, ransomware and state-sponsored campaigns; the paper argues for more regulatory convergence and defense-in-depth (Ikemefuna et al., 2025).

In particular, ICS and SCADA environments are very sensitive to human vulnerabilities. Operators continue to be a key weak point in the management of cyber-physical attacks, as was the case with the Ukrainian power outage (Sun et al., 2018). Surveys of legacy protocols like DNP3 and Modbus show that operators trust them and that attackers can leverage operator trust and lack of situational awareness to launch flooding or spoofing attacks (Zografopoulos et al., 2023). Smart grid research also shows that operator misinterpretation of complex attack signals may result in an escalation of persistent threats (Nafees et al., 2023). More broadly, the close cyber-physical coupling in SCADA generates novel vulnerabilities that cannot be addressed by conventional IT security without operator-centric approaches (Mo et al., 2011). Other research indicates that human vulnerabilities are increased by lack of training in emergency situations and cognitive overload at human-machine interfaces, reinforcing that human vigilance and resilience are critical factors in ICS cybersecurity (Khadka, & Ullah, 2025; Venkatachary et al., 2017).

Further, survey evidence has revealed human error to be a common cause of SCADA and CI incidents, with human operator misconfiguration and poor response associated with increasing system vulnerability (Miller and Rowe, 2012). More recent work on the Internet of Energy also emphasizes that operator over-reliance on automation and inappropriate human-machine interface management continue to leave distributed energy systems vulnerable to serious risks (Mogadem et al., 2022).

3.7.Summary of Findings

From the 40 papers that qualified, the synthesis reveals that employee awareness and training gaps are still a fundamental weakness, insider threats and negligence continue to play a significant role in incidents, and phishing and social engineering attacks continue to make up the majority of attack vectors. The study also demonstrated that compliance is a function of both individual motivation and organizational support, organizational culture is the key to embedding secure behavior and ICS/SCADA systems amplify the impact of human errors due to their complexity.

Together, these results demonstrate that human factors are not peripheral to cybersecurity resilience in the energy sector but central to it.

4. DISCUSSION

The synthesis of forty eligible studies shows that human factors are not add-on considerations but core vulnerabilities in the cybersecurity of energy infrastructures. When we look at awareness, training,

compliance and organizational culture, the evidence all points to the same pattern: employees are the targets and enablers of attacks. This section interprets these findings in the context of existing frameworks, compares findings across sectors and points to the gaps that still exist.

4.1.Persistent Awareness and Training Challenges

The reviewed studies indicate that awareness campaigns and training are still the mainstays of the solution, but are often ineffective. Kirlappos & Sasse (2011) demonstrated that employees often pass the test without changing their daily practices; Bada et al., (2019) determined that repeated initiatives do not result in measurable behavioral change. In the energy domain, Nazir et al., (2017) and Krause et al. (2021) validated that operator carelessness and lack of awareness were the main vulnerabilities in SCADA and smart grids.

By comparison, research in Industry 4.0 settings indicates that digital complexity is itself a magnifier of human vulnerabilities. Alqudhaibi et al., (2022) state that connected industrial systems lead to an increase in decision overload and human error. This indicates that the fast pace of digitalization of the energy sector, including renewable integration, could lead to an increase in awareness gaps, unless more agile training methods are implemented.

4.2.Insider Threats and Negligence as Recurring Risks

The insider threat was a universal finding. From SCADA incident investigations to surveys of oil and gas cyber-attacks, intentional insiders and careless employees consistently show up in incident investigations (Stergiopoulos et al., 2020). These results are consistent with the ICT literature in general, where employee error is also cited as a major facilitator of breaches (Alcaraz & Zeadally, 2015).

However, the causes are well known, but solutions are fragmented. Although there is growing evidence on the importance of human-centric security (Olubudo, 2024), there is a lack of evaluation of programmed effectiveness. This identifies a gap in the research around the measurement of long-term outcomes of insider threat mitigation strategies beyond short-term compliance with training.

These findings suggest that insider negligence is not only a technical failure but is typically a systemic failure. According to the analysis from DOE reports (Ajayi et al., 2025), human error cannot be eliminated even after implementing the advanced safeguards; therefore, technological advancements alone are not sufficient to reduce the risk of insiders. The Ukraine case (Clemente, 2018) also demonstrates how procedural weaknesses can be leveraged by attackers, consistent with other evidence that phishing and poor compliance are persistent vectors of entry (Wueest, 2014). Together these findings suggest that insider negligence is a convergence of poor training, poor process discipline and systemic over-reliance on technical defenses.

4.3.Social Engineering: The Dominant Human Exploit

Phishing and social engineering are the most common methods of exploiting human vulnerabilities. Wueest (2014) pointed out that targeted phishing attacks were the main entry points for adversaries in the energy industry. Similarly, Klimburg-Witjes and Wentland (2021) highlight the organizational narratives that portray employees in terms of deficient users, which not only obfuscate structural causes, but also simultaneously acknowledge the continuing vulnerability.

This result is not specific to energy. Reviews of water sector incidents also reported that attackers often gained access through a compromised employee account or by spoofing operators (Hassanzadeh et al., 2020). These parallels between sectors are a reminder that phishing and social engineering remain universal and unsolved human vulnerabilities across critical infrastructures.

As per the study conducted by Oluremi et al., (2025), phishing and other social engineering attacks are effective because they play on basic psychological motivators such as trust, fear, and urgency. This highlights the fact that employee susceptibility is a behavioral issue and not a technical one, and that awareness strategies need to be targeted within organizations.

4.4.Compliance and Organizational Support

The evidence shows that compliance is less a function of rules than of employee motivation and perceived organizational support. Protection motivation and deterrence theory (Herath & Rao, 2009) is adopted as a theoretical framework and the literature of MISQ stresses the importance of rationality-based beliefs (Bulgurcu et al., 2010).

This is similar to organizational culture models. Georgiadou et al. (2022) point out the existence of a culture of security as a prerequisite for the sustainable implementation of compliance. As the oil and gas industry has shown, training and compliance failures are just the tip of the iceberg underlying cultural gaps (Pothana et al., 2024). The evidence, therefore suggests that compliance needs to be embedded in organizational culture rather than left to individual responsibility.

The emerging EU approach focuses on the optimization of OT resilience rather than the prescription of specific technologies, placing power-sector cybersecurity in the wider context of regulatory tools on cross-border electricity flows (Toftegaard et al., 2024).

4.5.Organizational Culture and Security Environment

Culture was a recurring theme as a decisive factor. Parsons et al (2010) have recognized cultural and environmental mediation of security behavior and Georgiadou et al (2022) have suggested a systematic approach to the incorporation of security in everyday practices. In the context of renewable energy, Ekechukwu & Simpa (2024) directly related secure culture to investment sustainability and suggested that poor human practices jeopardize long-term viability.

Despite such popularity, there are gaps in operationalization of culture-based strategies. There is a gap in the literature in terms of providing practical models for measuring cultural change and relating cultural endeavors to reductions in incidents, and this is an important area for future empirical studies.

Kioskli et al. (2025) demonstrated that regulatory frameworks such as NIS2 place culture as a strategic pillar of cybersecurity, which further complements and reinforces previous arguments that organizational security cannot be built upon technical compliance. This is consistent with the cybersecurity culture framework of Georgiadou et al., (2022), which also argues that sustainable resilience relies on the inclusion of security values and behaviors as part of daily organizational practice.

4.6.ICS/SCADA-Specific Vulnerabilities and APTs

Results show that ICS and SCADA infrastructures are especially vulnerable to human error because of their socio-technical complexity. Nazir et al. (2017) highlighted operator error as one of the primary causes of SCADA failures and Hemsley & Fisher (2018) related human factors to cascading failures.

Advanced Persistent Threats (APTs) are an emerging threat that combines technical exploitation with human exploitation. APT campaigns are conducted using phishing, insider abuse and long-term persistence, explains Yusof (2024). These findings are consistent with the general findings in the literature that employee negligence leaves gaps for sophisticated and persistent adversaries (Al-Mhiqani et al., 2018).

The body of work presented in these studies illustrates that ICS and SCADA infrastructures are particularly vulnerable due to their close cyber-physical coupling and their dependence on human operators. Sun et al. (2017) illustrates how coordinated attacks such as the Ukrainian blackout capitalized on operator

vulnerabilities, and Mo et al. (2011) and Nafees et al. (2023) illustrate that conventional IT security approaches cannot account for situational awareness requirements on operators in such settings. Recent work on errors in emergency scenarios (Venkatachary et al., 2017) and the potential for cognitive overload to be exploited in human-machine interfaces (Khadka, & Ullah, 2025) also suggest that carelessness or misjudgment can amplify the effects of technical attacks. Together, the results indicate that resilience in ICS cybersecurity is as much a function of increasing human vigilance and preparedness as it is of fortifying technical defenses.

The data from (Miller & Rowe, 2012) supports operator error as a systemic rather than an incidental issue, as seen in most previous SCADA and CI incidents, and this issue is likely to be even more problematic on the Internet of Energy as increasing automation and distributed systems increase the risk of human-machine miscommunication slowing attack detection. Taken together, these works complement the case-based evidence by demonstrating that vulnerabilities are both historical and evolving and represent the need for continued attention to operator training and human-system interaction design. Existing standards and certifications are not sufficient for CPS safety on the IIoT scale and need specific technologies, better life-cycle management and harmonized security/safety regulation (Urquhart & McAuley, 2018).

4.7.Addressed Research Questions

This review answered the research questions by conducting a thematic synthesis of the studies included. RQ1 was answered by identifying a variety of human factor vulnerabilities in the energy industry that emerged across themes of awareness and training gaps, insider threats, social engineering, and specific ICS/SCADA weaknesses. RQ2 was answered with results on the impact of employee awareness, training and compliance and the limitations of awareness campaigns and the importance of policy adherence. RQ3 was captured in the themes of organizational culture and compliance, which illustrated how cultural and motivational factors influence secure or insecure behaviour. Comparative insights were also presented to RQ4, which demonstrated that energy infrastructures are vulnerable to the same types of vulnerabilities as seen in water, ICT, and Industry 4.0 contexts, but exacerbated by the socio-technical complexity of the sector. Finally, RQ5 was answered by identifying research gaps, in particular the lack of long-term training assessments, the lack of operationalization of security culture, and the lack of integration of human-centric defenses into emerging technologies.

4.8.Research Gaps and Future Directions

Despite advances, however, several gaps are evident throughout the reviewed works:

How awareness training affects you in the long run. Few studies test whether training programs maintain secure behavior over time. While studies have highlighted weaknesses of awareness programs, there are few studies that evaluate the effectiveness of awareness programs in the long run.

A human-centric security model should incorporate cognitive/behavioral understanding, attack techniques inventories and propose metrics (e.g. psychological ownership; security fatigue) and gamified training to mitigate susceptibility (Whitman et al. 2025).

How to operationalize security culture, although frameworks are available, empirical studies to quantify cultural transformation and its impact on incident reduction are missing.

Flexible strategies for digitalization. As Industry 4.0 and renewable integration grow, research needs to be done on how to prepare employees for the growing complexity of systems.

AI-powered awareness and support tools. While early research has indicated the potential of AI to assist employees in their decision-making (Pollini et al., 2022), the reality is still in the early stages.

Cross-sectoral application. Lessons from water, ICT and manufacturing must be systematically tested in the energy context to enhance transferability.

Four decades of research has shown that cybersecurity in the energy industry is ultimately a human issue as much as a technical one. As one study so aptly noted, employees are "the very entry points through which breaches occur" (Ghafir et al., 2018). Close these gaps not only through technical innovation but also with continuous cultural, behavioral and organizational transformation. By assembling the state of knowledge and mapping the path forward, this review will contribute to the building of a more resilient human-centric cybersecurity architecture for the energy sector.

5. PRACTICAL IMPLICATIONS

There are a number of implications for practice arising from this review. For energy companies, awareness programs need to shift from compliance-based training to behavioral science-based approaches that drive intrinsic motivation and long-term secure practices. Insider threat mitigation must be a combination of technical monitoring with targeted awareness programs that differentiate between careless and malicious behaviors. For policy makers and regulators, frameworks such as NIS2 and national energy security guidelines should be supported by mechanisms for measuring and enhancing organizational cybersecurity culture, so that policy is not limited to technical standards. An ICS and SCADA environment should include human-centered protections, in addition to technical protections, and should include training, organizational support and cultural initiatives for critical infrastructure operators. Finally, investment in renewable energy and Industry 4.0 systems needs to be complemented by workforce readiness, where human vulnerabilities are still the decisive factors in securing increasingly complex digital infrastructures.

6. LIMITATIONS

Although this review was conducted in a systematic manner and in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, some limitations are worth mentioning. First, the search range of studies included only articles published in English, which may have excluded relevant studies performed in other languages. Second, although the screening procedure involved 103 papers and resulted in a complete set of 40 eligible studies, the reliance on published and publicly available reports means that unpublished or proprietary industry research may not have been included.

Another limitation is the heterogeneity of included studies. The reviewed works differed in methodological rigor, industry focus and the level of detail regarding human factors, making comparison difficult. In particular, few studies have demonstrated longitudinal evidence on the long-term impact of awareness programs or organizational culture initiatives. Despite these limitations, the synthesis provides a systematic and transparent synthesis of existing knowledge and identifies important gaps in our understanding that require further research

7. CONCLUSION

In this systematic literature review, forty eligible studies and fifteen contextual works were synthesized to examine human factor vulnerabilities in energy industry cybersecurity, specifically employee awareness, training and behavior in preventing breaches. The results validate that human vulnerabilities-whether carelessness, non-compliance, or vulnerability to manipulation-are still the key facilitators of cyber-attacks in critical energy infrastructures.

The review makes three contributions:
Construction of fragmented knowledge by synthesizing research from the energy, oil and gas, renewable and critical infrastructure sectors, this paper offers the first integrated mapping of employee-related vulnerabilities in the energy sector.
Identification of thematic vulnerabilities Six themes were identified which were consistently found: awareness and training deficiencies, insider threats, social engineering, compliance failures, organizational culture, and ICS/SCADA-specific vulnerabilities. These categories can help frame thinking about and managing human factor risk.
Cross-sectoral learning. Comparative lessons from water, ICT and Industry 4.0 contexts show that human factors are common to all but are magnified by the socio-technical complexity of the energy industry.
This review makes a contribution to the literature by synthesizing a fragmented body of research on human factor vulnerabilities in cybersecurity in the energy industry, organizing the findings into six thematic categories and offering a comprehensive framework where employee awareness, behavior, and organizational culture emerge as key determinants of sector-wide resilience.

REFERENCES

1. Ajayi, O. O., Alozie, C. E., & Abieba, O. A. (2025). Enhancing cybersecurity in energy infrastructure: strategies for safeguarding critical systems in the digital age. Trends in Renewable Energy, 11(2), 201-212.
2. Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes, 50(2), 179-211
3. Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. International journal of critical infrastructure protection, 8, 53-66.
4. Al-Mhiqani, M. N., Ahmad, R., Yassin, W., Hassan, A., Abidin, Z. Z., Ali, N. S., & Abdulkareem, K. H. (2018). Cyber-security incidents: a review cases in cyber-physical systems. International Journal of Advanced Computer Science and Applications, 9(1).
5. Alqudhaibi, A., Aloseel, A., Jagtap, S., & Salonitis, K. (2022). Identifying and predicting cybersecurity threats in industry 4.0 based on the motivations towards a critical infrastructure. In Advances in Manufacturing Technology XXXV (pp. 10-16). IOS Press.
6. Asimiyu, Z. (2024). Cyber Threat Landscape for Critical Infrastructures: Management Tactics and Countermeasures.
7. Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. arXiv preprint arXiv:1901.02672.
8. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 523-548.
9. Clemente, J. F. (2018). Cyber security for critical energy infrastructure
10. Ekechukwu, D. E., & Simpa, P. (2024). The importance of cybersecurity in protecting renewable energy investment: A strategic analysis of threats and solutions. Engineering Science & Technology Journal, 5(6), 1845-1883.
11. 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

12. Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., ... & Baker, T. (2018). Security threats to critical infrastructure: the human factor. The Journal of Supercomputing, 74(10), 4986-5002.
13. Glenn, C., Sterbentz, D., & Wright, A. (2016). Cyber threat and vulnerability analysis of the US electric sector (No. INL/EXT-16-40692). Idaho National Lab.(INL), Idaho Falls, ID (United States).
14. 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), 03120003.
15. Hemsley, K. E., & Fisher, E. (2018). History of industrial control system cyber incidents (No. INL/CON-18-44411-Rev002). Idaho National Lab.(INL), Idaho Falls, ID (United States).
16. Herath, T., & Rao, H. R. (2009). Protection, motivation and deterrence: a framework for security policy compliance in organisations. European Journal of information systems, 18(2), 106-125.
17. Ikemefuna, Damian & Yusuf, Silvanus & Akinbi, Itiade. (2025). CYBERSECURITY CHALLENGES IN THE OIL AND GAS INDUSTRY: PROTECTING CRITICAL INFRASTRUCTURE FROM EMERGING THREATS. International Research Journal of Modernization in Engineering Technology and Science. 10.56726/IRJMETS61881.
18. Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: an interdisciplinary review and framework proposal. International Journal of Information Security, 24(3), 1-13.
19. Kioskli, K., Maglaras, L., Fotis, T., & Varouchas, E. (2025, July). Human Factors and Strategic Approaches in Cybersecurity: Threats for Critical Infrastructures in NIS2 Domains. In 16th International Conference on Applied Human Factors and Ergonomics (pp. 1-11). AHFE International.
20. Kirlappos, I., & Sasse, M. A. (2011). Security education against phishing: A modest proposal for a major rethink. IEEE Security & Privacy, 10(2), 24-32.
21. Klimburg-Witjes, N., & Wentland, A. (2021). Hacking humans? Social Engineering and the construction of the "deficient user" in cybersecurity discourses. Science, Technology, & Human Values, 46(6), 1316-1339.
22. Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021). Cybersecurity in power grids: Challenges and opportunities. Sensors, 21(18), 6225.
23. Lehto, M. (2022). Cyber-attacks against critical infrastructure. In Cyber security: Critical infrastructure protection (pp. 3-42). Cham: Springer International Publishing.
24. Line, M. B., Tøndel, I. A., & Jaatun, M. G. (2011, December). Cyber security challenges in Smart Grids. In 2011 2nd IEEE PES international conference and exhibition on innovative smart grid technologies (pp. 1-8). IEEE.
25. Manoharan, A., & Sarker, M. (2023). Revolutionizing cybersecurity: Unleashing the power of artificial intelligence and machine learning for next-generation threat detection. DOI: https://www. doi. org/10.56726/IRJMETS32644, 1.
26. Miller, B., & Rowe, D. (2012, October). A survey SCADA of and critical infrastructure incidents. In Proceedings of the 1st Annual conference on Research in information technology (pp. 51-56).
27. Mo, Y., Kim, T. H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2011). Cyber–physical security of a smart grid infrastructure. Proceedings of the IEEE, 100(1), 195-209.
28. Mogadem, M. M., Li, Y., & Meheretie, D. L. (2022). A survey on internet of energy security: related fields, challenges, threats and emerging technologies. Cluster Computing, 25(4), 2449-2485.
29. Mohammed, A. (2019). Ransomware in Critical Infrastructure: Impact and Mitigation Strategies. Journal of Innovative Technologies, 2(1).

30. Nafees, M. N., Saxena, N., Cardenas, A., Grijalva, S., & Burnap, P. (2023). Smart grid cyber-physical situational awareness of complex operational technology attacks: A review. ACM computing surveys, 55(10), 1-36.
31. Nazir, S., Patel, S., & Patel, D. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. Computers & Security, 70, 436-454.
32. Olubudo, Paul. (2024). Mitigating Insider Threats through Human-Centric Security Measures: A Review of Employee Training and Awareness Programs.
33. Oluremi, D., Vallabhaneni, R., Lallie, H., & Guglielmo, M., & Caporale. (2025). Abstract on Human Factors in Cybersecurity: Social Engineering and Insider Threats.
34. Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). Human factors and information security: individual, culture and security environment (No. DSTOTR2484).
35. Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. Computers & security, 31(4), 597-611.
36. Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. Cognition, Technology & Work, 24(2), 371-390.
37. Pothana, P., Gokapai, V., & Ramaseri-Chandra, A. N. (2024, October). Cybersecurity in the oil and gas sector: Vulnerabilities, solutions, and future directions. In 2024 Cyber Awareness and Research Symposium (CARS) (pp. 1-7). IEEE.
38. Pouraimis, G., Thanos, K. G., Grigoriadis, A., & Thomopoulos, S. C. (2019, May). Long lasting effects of awareness training methods on reducing overall cyber security risk. In Signal Processing, Sensor/Information Fusion, and Target Recognition XXVIII (Vol. 11018, pp. 201-211). SPIE.
39. Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. MIS quarterly, 757-778.
40. Pujari, S. R., & Hussain, M. A. (2024). Human Factor in Cybersecurity: Behavioral Insights into Phishing and Social Engineering Attacks. Nanotechnology Perceptions, 20, 630-642.
41. Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. Journal of Digital Forensics, Security and Law, 12(2), 8.
42. Stergiopoulos, G., Gritzalis, D. A., & Limnaios, E. (2020). Cyber-attacks on the oil & gas sector: A survey on incident assessment and attack patterns. Ieee Access, 8, 128440-128475.
43. Sun, C. C., Hahn, A., & Liu, C. C. (2018). Cyber security of a power grid: State-of-the-art. International Journal of Electrical Power & Energy Systems, 99, 45-56.
44. Ten, C. W., Manimaran, G., & Liu, C. C. (2010). Cybersecurity for critical infrastructures: Attack and defense modeling. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 40(4), 853-865.
45. Toftegaard, Ø., Grøtterud, G., & Hämmerli, B. (2024). Operational Technology resilience in the 2023 draft delegated act on cybersecurity for the power sector—An EU policy process analysis. Computer Law & Security Review, 54, 106034.
46. Tupa, J., Simota, J., & Steiner, F. (2017). Aspects of risk management implementation for Industry 4.0. Procedia manufacturing, 11, 1223-1230.
47. Urquhart, L., & McAuley, D. (2018). Avoiding the internet of insecure industrial things. Computer law & security review, 34(3), 450-466.

48. 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.
49. Whitman, John & El-Karim, Aisha & Nandakumar, Priya & Ortega, Fernando & Zheng, Lijuan & James, Andrew & Bua, Nelson. (2025). Human-Centered AI Security: Combating Social Engineering in Intelligent Critical Infrastructure Networks.
50. Wueest, C. (2014). Targeted attacks against the energy sector. Symantec. Security Response.
51. Yusof, Z. B. (2024). Exploration of advanced persistent threats: techniques, mitigation strategies, and impacts on critical infrastructure. International Journal of Advanced Cybersecurity Systems, Technologies, and Applications, 8(12), 1-9.
52. 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.