DOI: 10.2478/ijasitels-2024-0017

Explore the intersection of Self-Determination Theory and cybersecurity education - A literature review

Iulia Feraru[1], *Laura Bacali*[2]

1 IOSUD,, Technical University of Cluj-Napoca, Memorandumului 28, 400114, ClujNapoca, Romania

2 Technical University of Cluj-Napoca, Memorandumului 28, 400114, ClujNapoca, Romania

Abstract

This paper explores how organizations can create a sustainable, security-first culture in an increasingly complex environment where organizational and national cultures are strong influencing factors in human behaviour. In cybersecurity education, as in any effort of education, there must be a principled commitment to long-term behaviour modification through intrinsic motivation, foundational to employees acting consistently in secure ways. The review of the literature falls squarely within Self-Determination Theory, underlining the pertinence of autonomy, competence, and relatedness as distinctive factors in cybersecurity education, highlighting that these constructs are necessary at all levels for perpetual security and compliance.

The results indicated that an effective security-first culture could only emerge when cybersecurity formed part of the core values and practices within organizations. It also explained that leadership styles, such as transformational and servant leadership, play an important role in the development of intrinsic motivation by fostering trust, empowerment, and a sense of shared responsibility. It also highlights how national cultural dimensions, such as individualism and power distance, may change how differently oriented employees respond to cybersecurity policies and practices. Approaches to cybersecurity education should be tailored to both organizational and national cultural factors to develop cybersecurity education strategies that could go beyond mere compliance and build a proactive security mindset.

This is important because it underlines how the SDT acts as a framework for understanding how companies could help foster a security-first culture that, at the same time, will create sustainable, resilient, and intrinsically driven cybersecurity behaviours among employees.

Keywords: Behavioural change, information security, organizational culture, national culture, Self-Determination Theory

1 Introduction

Information security has become a critical concern for organizations across the globe, as the protection of sensitive information is fundamental to maintaining trust, ensuring regulatory compliance, and safeguarding against reputational and financial losses. Despite the continuous advancement of technical security measures, such as next-generation antivirus solutions and sophisticated threat detection systems, the human element remains the most significant vulnerability in information security. In the era of

Industry 4.0 ([8] Bhaharin et al., 2019), human error remains a significant threat to information security, often resulting from negligence, ignorance, and failure to adhere to organizational information security policies. To increase compliance with information security policies (ISPs) and reduce security incidents related to human behaviour, it is essential to systematically analyse and address the underlying issues influencing employees' attitudes towards policy adherence ([8] Bhaharin et al., 2019). Motivation is a critical component in shaping secure behaviour and ensuring compliance with security policies. According to Self-Determination Theory (SDT) ([75] Deci & Ryan, 2000), intrinsic motivation—driven by a sense of autonomy, competence, and relatedness—can significantly enhance employees' commitment to security practices ([75] Deci & Ryan, 2000). However, motivation is not solely an individual attribute but is also influenced by the broader cultural context within which individuals operate. Both organizational culture and national culture play very important roles in shaping employees' attitudes, behaviours, and motivations toward information security.

The interaction between organizational culture and national culture is a complex area of study, as cultural factors can either support or hinder the adoption of secure behaviours. Organizational culture encompasses shared values, norms, and practices that influence how employees perceive and respond to security policies ([10] Schein et al, 2017). Leadership, communication, and trust within an organization are key aspects that can either foster a security-conscious culture or contribute to complacency and non-compliance ([10] Schein et al, 2017). On the other hand, national culture, as defined by Hofstede's dimensions, affects individuals' perceptions of authority, risk, and responsibility, which in turn influences their willingness to engage in security practices ([9] Hofstede et al, 2005).

The research question (RQ) formulated to explore these dynamics was:

- RQ: How can organizations foster a security-first culture that enhances employees' intrinsic motivation and sense of shared responsibility?

This article is aiming to investigate how intrinsic motivation, driven by the principles of Self-Determination Theory (SDT) ([75] Deci & Ryan, 2000), can support lasting behaviour change in cybersecurity. Motivation itself is a complex construct, encompassing both extrinsic and intrinsic forms. The BJ Fogg Behaviour Model ([5] Fogg, 2009) highlights that behaviour arises from the convergence of motivation, ability, and triggers, suggesting that motivation is essential for sustainable security compliance. While extrinsic motivators, such as penalties or rewards, can prompt compliance, they often lack the staying power required for deep-rooted behavioural change.

This article aims to shed light on how SDT constructs can be worked with to drive intrinsic motivation and achieve sustainable behaviour change, thus positioning cybersecurity as a core component of organizational culture rather than an obligatory task. By creating and maintaining an environment where individuals feel autonomous, competent, and connected, organizations can build a foundation for continuous cybersecurity education and proactive security engagement.

2 Background

2.1 Information security

Information security is a concept that becomes ever more enmeshed in many aspects of our society, largely as a result of our nearly ubiquitous adoption of computing technology. In our everyday lives, many of us work with computers for our employers, play on computers at home, go to school online, buy goods from merchants on the Internet, take our laptops to the coffee shop and check our e-mail, carry our smartphones on our hips and use them to check our bank balances, track our exercise with sensors in our shoes, and so on, ad infinitum. ([1] Andress, J.,2014)

There are various definitions of Information Security and they all relate to the preservation of confidentiality, integrity and availability of information over the Internet and other properties, such as authenticity, accountability, non-repudiation and reliability that can also be involved. ([2] ISO/IEC 27000:2018)

Information is a critical business asset nowadays and managing its security ensures business continuity, competitiveness, profitability, prestige, elimination of threats and losses resulting from realized risks. ([3] Bolek et. al, 2023)

2.2 Human-centric security

Although technical security controls, such as next-generation antivirus software and improved spam filters, continue to advance, the human factor remains the leading cause of security incidents, contributing to 68% of data breaches. ([4] Verizon, 2024)

Human error, negligence, and risky behaviour contribute significantly to security incidents, often cancelling even the most sophisticated technical defences. Recognizing this, there is an increasing need to focus on understanding the role of individuals in maintaining information security. Employees, when properly educated and motivated, can become the organization’s strongest line of defence. By fostering a culture of awareness and proactive response to potential threats, organizations can significantly reduce the likelihood of data breaches and security violations. This highlights the importance of examining behaviour in the context of information security, as it is through shaping secure behaviours that organizations can transform their employees from potential risks into active participants in safeguarding sensitive information.

2.2.1 Human behaviour in information security

Understanding human behaviour is crucial in the field of information security, as employees' actions can either enhance or undermine an organization’s security posture. Factors such as awareness, motivation, and the ability to recognize and respond to security threats play a critical role in shaping secure behaviour. To explore how behaviour can be influenced and improved, theoretical models of behaviour change provide valuable insights. One such model is the Fogg Behaviour Model ([5] Fogg, 2009), developed by Dr. BJ Fogg, which offers a framework for understanding how behaviours are formed. At its core, the model suggests that three key elements must converge simultaneously for a behaviour to occur: motivation, ability, and prompts. Specifically, if a behaviour is sufficiently motivated, easy to perform, and triggered appropriately, it is more likely to occur. Conversely, if any of these elements are lacking or misaligned, behaviour change is less likely to happen.

2.2.2 Motivation

Motivation plays a central role in shaping employees' adherence to information security policies and practices. A well-established framework for understanding motivation is Self-Determination Theory (SDT), ([6] Deci et. al, 2013), developed by Deci and Ryan in the 1980s, which distinguishes between intrinsic and extrinsic motivation. Intrinsic motivation refers to performing an action because it is inherently satisfying or enjoyable, while extrinsic motivation involves performing actions to achieve external rewards or avoid negative consequences. In the context of information security, fostering intrinsic motivation can be highly effective, as it encourages employees to adopt secure behaviours because they personally value the importance of protecting organizational assets.

SDT ([6] Deci et. al, 2013) posits that three key psychological needs must be fulfilled to foster intrinsic motivation: autonomy, competence, and relatedness. When employees feel autonomous, competent, and connected to others, they are more likely to internalize security practices and consistently comply with security policies. Recent studies have shown that autonomy and competence, in particular, significantly influence employees' intentions to follow security guidelines, emphasizing the need to create environments where employees feel capable and in control of their security-related decisions ([7] Gangire et. al, 2021).

The three constructs of the Self-Determination Theory (autonomy, competence and relatedness) do not operate in isolation. The broader organizational culture plays a pivotal role in either supporting or hindering the fulfilment of these psychological needs. Moreover, national culture affects how employees perceive authority, risk, and individual responsibility within the workplace.

2.3 Organizational culture

Organizational culture refers to the shared values, beliefs, norms, and practices that shape the behaviour and attitudes of employees within an organization. It serves as the foundation for how individuals interact with one another and how they approach their work, influencing everything from decision-making processes to responses to challenges and opportunities ([10] Schein et al, 2017). In the context of information security, organizational culture plays a significant role in determining how security policies are perceived and adhered to by employees. A positive and supportive culture can foster a security-first mindset, while a toxic or indifferent culture may lead to negligence and increased vulnerability to security breaches.

Leadership is a critical element of organizational culture that significantly shapes the security behaviours of employees. Effective leadership can motivate and inspire employees to adhere to security policies and engage in secure practices. Various leadership styles, such as transformational, transactional, and participative leadership, have different impacts on information security compliance. Transformational leaders, in particular, encourage a proactive security culture by fostering trust, organizational justice, and a shared commitment to security goals. They inspire employees to go beyond mere compliance and actively engage in protective behaviours, whereas transactional leaders tend to emphasize compliance through a system of rewards and penalties ([11] Sürücü, 2021).

Communication within an organization is important for promoting awareness and understanding of information security policies. It serves as the channel through which security expectations, procedures, and the rationale behind policies are conveyed to employees. Effective communication ensures that employees are not only aware of security policies but also understand their importance and relevance to their daily work.

Trust is a foundational element of organizational culture that influences how employees perceive and respond to security policies. Trust in leadership, peers, and the organization itself can significantly impact employees' willingness to follow security protocols and report incidents without fear of retribution. A high level of trust within an organization encourages employees to take security responsibilities seriously and to collaborate openly in identifying and mitigating risks.

2.4 National culture

National culture refers to the shared values, beliefs, norms, and behaviours that are characteristic of a particular country or society ([9] Hofstede et.al, 2005). It shapes individuals' attitudes, perceptions, and actions, influencing how they interact with authority, handle uncertainty, and respond to organizational policies, including information security protocols. Understanding the impact of national culture on information security behaviour is essential for multinational organizations seeking to implement effective security strategies across different cultural contexts. By recognizing the cultural nuances that affect employees' motivations and compliance behaviours, organizations can tailor their security policies to better align with local cultural values.

2.5 Compliance with Information Security Policies (ISPs)

Research indicates that fostering a security-aware culture that emphasizes the three psychological needs (autonomy, competence and relatedness) described by the Self-Determination Theory (SDT) ([6] Deci et. al, 2013) can significantly enhance employees' motivation to follow security protocols. For example, organizations that provide regular training and support can help employees feel more competent in managing security threats. Similarly, creating an environment where employees feel a sense of ownership over security processes can satisfy their need for autonomy, leading to greater intrinsic motivation to comply with ISPs ([8] Bhaharin et al., 2019).

Organizational culture, leadership and national culture significantly impacts how employees perceive and react to information security policies. To enhance compliance with ISPs, organizations must integrate these cultural insights with principles from SDT ([6] Deci et. al, 2013). By creating environments that satisfy employees’ psychological needs for autonomy, competence, and relatedness, organizations can foster intrinsic motivation for security compliance across diverse cultural contexts. For example, in a Clan culture ([76] Cameron et al.,2006), emphasizing shared responsibility and collective rewards can satisfy relatedness and competence, leading to voluntary compliance. In a Hierarchy culture ([76] Cameron et al.,2006), providing clear guidelines and consistent feedback can satisfy competence, while offering employees some control over how they implement security measures can fulfil their need for autonomy.

3 Review method

This systematic literature review (SLR) follows a rigorous process to ensure a consistent and transparent analysis of existing research on the intersection of Self-Determination Theory (SDT) and cybersecurity education. The methodology was guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) ([14] PRISMA, 2020) framework and the Joanna Briggs Institute (JBI) guidelines ([15] JBI, 2020), while also incorporating elements of the Evidence-Based Software Engineering (EBSE) guidelines ([13] Kitchenham et al., 2007). This section outlines the research protocol, including the research questions, search strategy, inclusion and exclusion criteria, data extraction process, and the synthesis of the findings.

3.1 Review protocol and research question

A review protocol was developed to ensure consistency and reproducibility throughout the review process. The protocol outlined the following key elements:

- Research aim: To explore how SDT constructs (autonomy, competence, and relatedness) foster long-term behaviour change, and thus cybersecurity education, through the use of intrinsic motivation.
- Research question (RQ): to address how organizations can foster a security-first culture that enhances intrinsic motivation.

RQ: How can organizations create a security-first culture that increases employees' intrinsic motivation and sense of shared responsibility towards Information Security, thereby promoting compliance with security policies?

This fourth question is designed to explore the critical intersection between organizational culture, motivation, and employee behaviour in the field of information security. The question reflects a shift from purely technical approaches to cybersecurity toward a more holistic view that emphasizes human factors and organizational dynamics. By focusing on intrinsic motivation—rooted in the Self-Determination Theory (SDT)—the question seeks to understand how internal drivers like autonomy, competence, and relatedness can encourage proactive security behaviours. The focus is on relatedness, examining how a sense of shared responsibility within an organization can cultivate a collective approach to protecting information assets.

The systematic literature review was conducted in 4 stages as described in Fig.1. The stages are described in detail in the next sections.

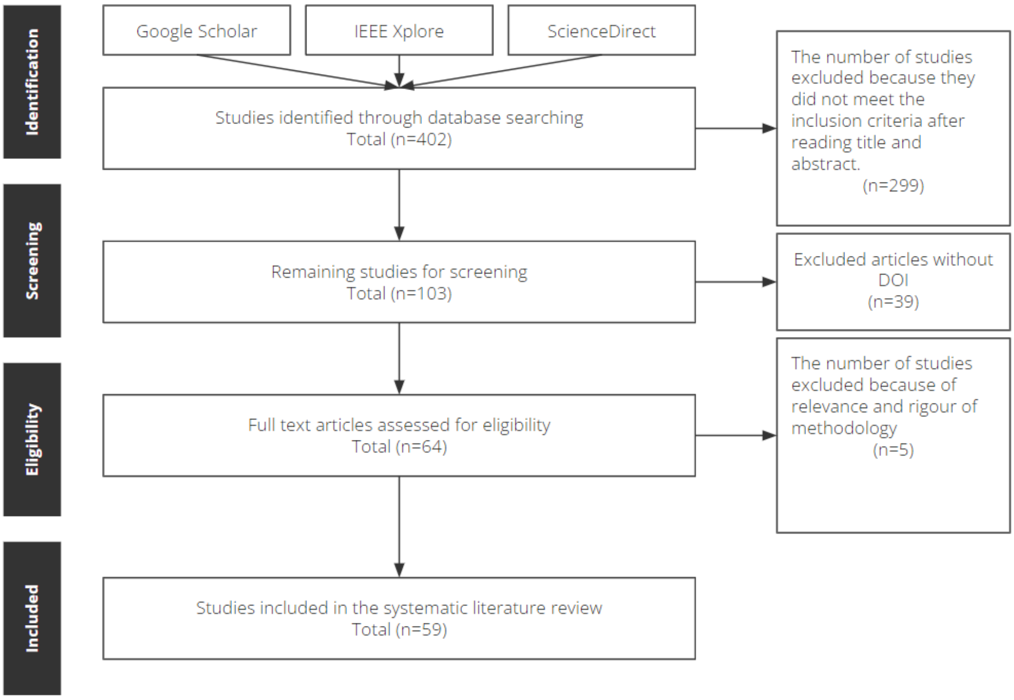
Identification
Screening
Eligibility
Included
Google Scholar
IEEE Xplore
ScienceDirect
Studies identified through database searching
Total (n=402)
The number of studies excluded because they did not meet the inclusion criteria after reading title and abstract.
(n=299)
Remaining studies for screening
Total (n=103)
Excluded articles without DOI
(n=39)
Full text articles assessed for eligibility
Total (n=64)
The number of studies excluded because of relevance and rigour of methodology
(n=5)
Studies included in the systematic literature review
Total (n=59)

Fig.1 PRISMA Flow Diagram

3.1.1 Identification

The initial search was conducted across multiple databases, including Google Scholar, IEEE Xplore, and ScienceDirect, using the search strings identified for each Research Question. The search resulted in 402 studies. These studies included a mixture of research articles, review articles, conference papers, and theses, reflecting the interdisciplinary nature of the topic and the broad scope of the search strategy. The first stage involved an initial screening of titles and abstracts of all studies identified during the search phase. This step aimed to quickly eliminate studies that were clearly irrelevant to the research questions or outside the scope of the review.

The search strings were designed to include key terms without complex Boolean operators in Google Scholar, while more refined Boolean logic was used in Scopus and IEEE Xplore. Below are the detailed search strings developed for each area of focus:

- *"information security compliance" AND “employee motivation” AND “security policies"*
- *"security behaviour" AND "information security policies" AND “adherence”*
- *"security awareness" AND "employee motivation" AND "information security compliance"*
- *"security policy adherence" AND "behavioural intention" AND "organisational culture"*
- *"information security" AND "compliance behaviour" AND "employee engagement"*
- *"shared responsibility" AND "information security" AND "employee behaviour"*

- *"security-first culture" AND "intrinsic motivation" AND "compliance"*

"collective responsibility" AND "information security" AND "engagement"

3.1.2 Screening

103 studies were retained for further review if they included any relevant keywords related to organizational culture, leadership, national culture, motivation, or information security compliance.

3.1.3 Full text review

Studies that passed the initial screening were subjected to a full-text review to assess their relevance. Each study was evaluated against the predefined inclusion and exclusion criteria, ensuring they addressed one or more of the research questions comprehensively. 64 studies were retained.

Table 1. Inclusion and Exclusion Criteria for the studies

Inclusion Criteria	***Inclusion Criteria***
Studies published in peer-reviewed journals and conference proceedings.	Studies focusing solely on technical aspects of information security without considering human or cultural factors.
Studies published between 2013 and 2024.	Studies not aligned with the research questions or lacking empirical data or theoretical analysis.
Studies available in English.	Non-English studies.
Studies accessible in full-text format.	Studies not available in full-text or behind a paywall without accessible alternatives.
Studies addressing the relationship between organisational culture, national culture, leadership, motivation, and information security compliance.	Studies without a DOI number.

3.1.4 Study quality assessment

In accordance with the PRISMA 2020 and Joanna Briggs Institute (JBI) guidelines, a rigorous quality assessment was conducted for all 64 studies included in this systematic review. The goal of the assessment was to ensure that only methodologically sound studies were retained for synthesis, thereby enhancing the reliability and validity of the review findings.

The quality assessment was based on criteria like clarity and transparency, data analysis techniques, data collection methods and sample size and relevance. A Keep or Discard decision was made for each study, depending on whether it met the methodological standards necessary to ensure reliability. Studies that exhibited significant methodological weaknesses (n=5) —such as inadequate sample sizes, unclear data collection methods, or lack of transparency in reporting—were excluded from further analysis.

The final set of studies included in the systematic review were those that met all inclusion criteria, passed the quality assessment, and provided relevant and rigorous contributions to the research questions.

This set of studies forms the basis for the subsequent data extraction and synthesis phases, ensuring an evidence-based understanding of the impact of cultural and leadership factors on information security compliance.

3.2 Data extraction

The data extraction process was designed to systematically capture relevant information from the 59 studies retained after the study quality assessment. The goal of this process is to ensure that all data relevant to the research questions is consistently and accurately recorded, allowing for comprehensive synthesis and analysis in subsequent stages. A standardized data extraction form was created using Google Sheets, enabling the organization and management of data across all studies in a structured manner. This format ensured transparency, traceability, and ease of access throughout the review process.

The data extraction form included the following key fields and extraction criteria, presented in Table 2.

3.3 Data synthesis

The data synthesis for this systematic literature review was planned in alignment with the data extraction process, as outlined in the previous section. Each of the 59 selected studies was reviewed to extract relevant information based on the key fields: research design, sample, research objectives, data collection methods, key findings, and relevance to the research question (RQ). The synthesis strategy follows the structure of the research questions, integrating findings across these thematic areas.

Given the interdisciplinary nature of this review, the synthesis is organized into two phases. First, a general overview of how the studies relate to the core themes of intrinsic motivation and security-first culture is presented. Then, the synthesis looks into more specific aspects tied to each of the SDT constructs (autonomy, competence, relatedness), providing a coherent analysis of how each study addresses these core constructs.

Table 2. Data Extraction Form Columns

Item	***Description***
Study identifier	
Year	Year of publication
Author	Author(s) of literature
Title	Title of the study
Study characteristics	
Research design	Study type (qualitative, quantitative, mixed methods)
Sample	Sample size and context
Research objectives	The aims or hypotheses of the study
Data collection methods	Surveys, interviews, case studies,

	literature review etc.
Key findings	Summary of the main results or conclusions of the study
Relevance to RQs	Indicate which of the RQs the study addresses
RQ Security culture and intrinsic motivation	Collect data on practices and strategies that promote a security-first culture and increase intrinsic motivation (aligning with Self-Determination Theory) and shared responsibility.

The synthesis of the 59 papers shows that competence and relatedness are key to promoting security compliance, with autonomy playing a lesser but supportive role. Competence is strengthened through training that builds necessary skills and confidence in handling security tasks, while relatedness, fostered by social norms and a supportive culture, instill a sense of shared responsibility. Though autonomy is less emphasized, allowing some discretion in security practices can increase intrinsic motivation. Together, these elements create a more engaged and resilient organizational approach to cybersecurity.

4 Results

The collection of the 59 selected studies includes a broad range of research addressing how organizational, leadership, and cultural factors influence information security behaviours. These studies investigate critical dimensions such as the creation of a security-first culture, the role of intrinsic motivation in fostering security compliance, and the impact of both organizational and national culture on employee behaviour.

The selected studies cover multiple domains, with several focusing on the influence of leadership style, communication, national cultural dimensions, on security practices and policy compliance. Additionally, a significant portion of the research explores how shared responsibility and intrinsic motivation can enhance adherence to Information Security Policies. This diverse body of literature offers an increased perspective on human factors affecting information security across different organizational contexts.

The studies span across various geographical regions, providing a global perspective on information security practices, with a majority in the Western cultures (13% in US and 32% in Europe). The geographical breakdown, based on the lead author's affiliation or the main geographical focus of the analysis, is presented in Table 3.

This geographic diversity enriches the study by incorporating cross-cultural insights and varied approaches to security practices and policy compliance.

The selected studies were published between 2014 and 2024, with a majority concentrated in recent years, particularly between 2019 and 2024. This distribution, presented in Fig.2, highlights an increasing academic interest in the intersection of culture and information security during this period. The continuous rise in publications reflects the growing recognition of cultural and human factors as critical elements in enhancing security practices.

4.1 RQ: How can organisations create a security-first culture that increases employees' intrinsic motivation and sense of shared responsibility towards Information Security, thereby promoting compliance with security policies?

Creating a security-first culture involves fostering intrinsic motivation, where employees feel personally responsible for the security of the organization. Multiple studies suggest that intrinsic motivation is more effective than extrinsic motivators like rewards or sanctions in promoting long-term compliance ([19] Kuo et.al (2020), [24] Sherif et. al. (2015),[31] Chaudhary, S. (2024)). [19] Kuo et.al (2020) found that while deterrence can enforce compliance, intrinsic motivation—driven by personal responsibility and security awareness—leads to sustainable security behaviours, as employees internalize security values and practices.

Security training and awareness programs were identified as key mechanisms for cultivating intrinsic motivation ([31] Chaudhary, S. (2024), [20] Chaudhary et.al. (2023), [36] AITooq et. al. (2024), [44] Hakami et. al. (2022)). [31] Chaudhary, S. (2024) emphasized that continuous, engaging, and tailored security training helps create a sense of responsibility among employees, making them more likely to adhere to security policies. Similarly, [20] Chaudhary et.al. (2023) noted that in small and medium-sized enterprises, tailored training programs that align with the company's culture are essential for fostering a security-first mindset. This personalization of training content helps employees see the relevance of security measures in their daily work and strengthens their commitment to secure practices.

Table 3 Geographical distribution of papers

Region	% of Papers	Papers
Asia	22.03%	[19] Kuo et.al (2020), [23] Chu et.al. (2019), [27] Palanisamy et. al. (2020), [29] Handri et. al. (2024), [38] Balagopal et. al. (2024), [45] Sari et. al. (2022), [48] Angraini et. al. (2019), [52] Purnomo et.al. (2024), [56] Pham et. al. (2017), [59] Mubarkoot et. al. (2023), [61] Puspadevi Kuppusamy et. al. (2020), [63] Suranto et. al. (2022), [66] Liu et. al. (2022)
Brazil	5.08%	[25] dos Santos Vieira et. al. (2022), [54] Iwaya et. al. (2022), [55] Apolinário et. al. (2023)
Europe	32.20%	[20] Chaudhary et.al. (2023), [21] Prümmer et.al. (2024), [22] Orehek et. al. (2020), [24] Sherif et. al. (2015), Chaudhary, S. (2024), [33] Riahi et. al. (2024), [35] Khando et. al. (2024), [40] Badie' Alhmoud et. al (2024), [42] Woods et. al. (2024), [47] Rocha Flores et. al. (2014), [49] Shaikh et. al. (2023), [50] Ameen et. al. (2021), [51] Yeng et. al. (2021), [57] Borgert et. al. (2024), [58] Rocha Flores et. al. (2016), [60] Paananen et. al. (2020), [62] Marsh et. al. (2022), [70] Karjalainen et. al. (2020), [72] Murray et. al. (2024)
Middle East	10.17%	[30] Sany et. al. (2022), [36] AITooq et. al. (2024), [37] Baomar et. al. (2024), [39] Alassaf et. al. (2021), [44] Hakami et. al. (2022), [68] Zyoud et. al. (2024)

Oceania	11.86%	[18] Skinner et.al. (2019), [34] Reeves et. al. (2021), [46] AlGhamdi et. al. (2020), [53] Wiley et. al. (2020), [64] Tam et. al. (2021), [69] Moustafa et. al. (2021), [71] Sutton et. al. (2024)
Others	5.08%	[26] Aksoy (2024), [41] Lubua et. al. (2023), [43] Mashiane et. al. (2021)
US	13.56%	[16] Shah et.al.(2023), [17] Taherdoost (2024), [28] Alowais et. al. (2023), [32] Vance et. al. (2020), [65] Petrič et. al. (2022), [67] Hoffman et. al. (2020), [73] Chen et. al. (2022), [74] Sahin et. al. (2024)

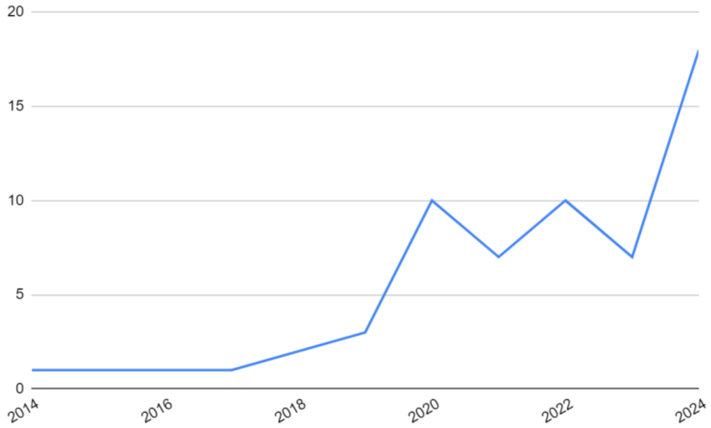

Figure 2 The year of publication of studies

Leadership also plays a role in promoting intrinsic motivation through role modelling and creating an inclusive security culture ([37] Baomar et. al. (2024), [24] Sherif et. al. (2015)). [37] Baomar et. al. (2024) demonstrated that transformational leadership encourages a security-first culture by engaging employees in security initiatives and making them feel valued in the organization's security efforts. Such leadership not only models secure behaviour but also fosters a supportive environment where employees feel their contributions to security are recognized and valued.

[40] Badie’ Alhmoud et. al. (2024) expands on this by discussing the role of servant leadership in fostering a security-first culture. Servant leaders, who prioritize the well-being and development of their employees, help create an environment where employees feel trusted and supported in their security roles. [40] Badie’ Alhmoud et. al. (2024) highlights that when employees feel that leadership genuinely cares about their professional growth and ethical well-being, they are more inclined to internalize security behaviours as part of their intrinsic motivation.

[42] Woods et. al. (2024) highlights the importance of empowerment in a security-first culture. By granting employees autonomy and allowing them to take ownership of security-related tasks, organizations can foster intrinsic motivation. [42] Woods et. al. (2024) suggests that autonomy in decision-making around security policies helps employees feel more responsible and committed to maintaining security standards, as they see these responsibilities as integral to their role within the organization.

In addition, [48] Angraini et. al. (2019) emphasizes the significance of competence-building through regular skill development and training. When employees feel competent in their security tasks, they are more confident and motivated to engage in secure behaviours. [48] Angraini et. al. (2019) found that employees who receive consistent, high-quality training feel empowered to take proactive measures, viewing security as an area where they can excel and contribute positively to the organization.

[59] Mubarkoot et. al. (2023) and [66] Liu et. al. (2022) provide insights into relatedness as a factor in creating a security-first culture. [59] Mubarkoot et. al. (2023) found that fostering a sense of belonging and shared responsibility in security practices enhances employees' intrinsic motivation. When employees perceive security as a collective goal shared with their peers, they feel more accountable and are more likely to adopt secure behaviours. Similarly, [66] Liu et. al. (2022) emphasizes that a culture of open communication and mutual respect, driven by servant leadership, can increase the sense of relatedness among employees, making security practices feel like a joint effort rather than an individual obligation.

This discussion of intrinsic motivation links closely to the constructs of Self-Determination Theory (SDT)—Relatedness, Competence, and Autonomy—which are essential for a robust security culture. To foster a security-first culture, understanding how different motivational constructs of SDTare addressed in the literature is essential. These constructs each play a role in motivating employees to adhere to security practices. The distribution of papers across these constructs reflects varying emphases, with some studies focusing exclusively on a single construct, while others examine the interplay between two or all three.

- **Competence**

The Competence construct, addressed alone in papers like [18] Skinner et.al. (2019), [21] Prümmer et.al. (2024), [39] Alassaf et. al. (2021) emphasizes the need for employees to feel skilled and capable in managing security tasks. These studies highlight the importance of training and support in building employees' confidence in their ability to handle security responsibilities effectively. For example, [18] Skinner et.al. (2019) demonstrates that competency-building programs, such as ongoing security training, help employees develop the skills needed to follow security protocols confidently.

- **Relatedness**

Papers that exclusively focus on Relatedness—such as [16] Shah et.al.(2023) and Vance et. al. (2020)—underscore the importance of social connections and a sense of belonging in promoting security behaviours. These studies highlight how fostering a supportive social environment within the organization can motivate employees to adhere to security protocols. [16] Shah et.al.(2023) specifically discusses how team cohesion leads to a collective responsibility for security, which enhances adherence to security policies.

- **Autonomy and Competence**

Papers like [34] Reeves et. al. (2021), [42] Woods et. al. (2024) and [74] Sahin et. al. (2024) focus on both Autonomy and Competence, indicating that empowering employees while also ensuring they feel competent can foster a proactive approach to information security. For instance, [34] Reeves et. al. (2021) finds that when employees feel both skilled and autonomous, they are more likely to take personal responsibility for security actions, which helps reduce vulnerabilities due to human error.

- **Autonomy and Relatedness**

Studies such as [23] Chu et.al. (2019) and [73] Chen et. al. (2022) address Autonomy and Relatedness together, examining how a sense of belonging coupled with autonomy can foster intrinsic motivation. **[23]** Chu et.al. (2019) highlights that when employees feel connected to their colleagues and are empowered to make security decisions, they are more likely to internalise security practices, making them a part of their daily responsibilities.

- **Competence** and **Relatedness**

The pairing of Competence and Relatedness is more commonly explored, with studies emphasising the importance of employees feeling both connected to their peers and skilled in security tasks. 19 papers address this pairing: [17] Taherdoost (2024), [19] Kuo et.al (2020), [22] Orehek et. al. (2020), [24] Sherif et. al. (2015), [25] dos Santos Vieira et. al. (2022), [26] Aksoy (2024), [28] Alowais et. al. (2023), [30] Sany et. al. (2022), [36] AITooq et. al. (2024), [38] Balagopal et. al. (2024), [40] Badie' Alhmoud et. al. (2024), [41] Lubua et. al. (2023), [44] Hakami et. al. (2022), [48] Angraini et. al. (2019), [55] Apolinário et. al. (2023), [47] Rocha Flores et. al. (2014), [59] Mubarkoot et. al. (2023), [65] Petrič et. al. (2022) and [66] Liu et. al. (2022). These papers suggest that a culture that promotes both social bonds and competency development can significantly improve compliance with security protocols. [17] Taherdoost (2024), for instance, notes that when employees feel both competent and supported by their peers, they are more motivated to adhere to security guidelines, as they perceive these behaviours as collectively valued within the organization.

- **Intersection of all three constructs**

The largest number of papers (29) address the combined influence of Relatedness, Competence, and Autonomy: [27] Palanisamy et. al. (2020), [29] Handri et. al. (2024), [31] Chaudhary, S. (2024), [33] Riahi et. al. (2024), [35] Khando et. al. (2024), [37] Baomar et. al. (2024), [43] Mashiane et. al. (2021), [45] Sari et. al. (2022), [46] AlGhamdi et. al. (2020), [47] Rocha Flores et. al. (2014), [49] Shaikh et. al. (2023), [50] Ameen et. al. (2021), [51] Yeng et. al. (2021), [52] Purnomo et.al. (2024), [53] Wiley et. al. (2020), [54] Iwaya et. al. (2022),[56] Pham et. al. (2017), [57] Borgert et. al. (2024), [60] Paananen et. al. (2020), [61] Puspadevi Kuppusamy et. al. (2020), [62] Marsh et. al. (2022), [63] Suranto et. al. (2022), [64] Tam et. al. (2021), [67] Hoffman et. al. (2020), [68] Zyoud et. al. (2024), [69] Moustafa et. al. (2021), [70] Karjalainen et. al. (2020), [71] Sutton et. al. (2024), [72] Murray et. al. (2024). These studies advocate for a holistic approach, suggesting that when employees feel competent, connected, and autonomous, they are intrinsically motivated to engage in secure behaviours. [27] Palanisamy et. al. (2020), for example, provides insights into how organizations that foster a supportive environment, build necessary skills, and empower employees see higher levels of compliance and proactive security practices. This intersection suggests that the most effective security-first cultures are those that integrate all three constructs, providing employees with the social support, skills, and independence they need to adhere to security practices consistently.

Summary of key findings

Across all research questions, the literature reveals that organizational culture, leadership, and national cultural dimensions are integral to fostering a security-first mindset. Communication, trust, and organizational norms are key components of a strong security culture, while leadership plays a critical role in motivating employees to engage with security practices. National culture influences how employees perceive and respond to security policies, with collectivist cultures and high uncertainty-avoidance cultures showing higher compliance rates. Finally, the review suggests that organizations that successfully integrate security into their core values through education, leadership support, and shared responsibility see higher levels of policy compliance.

5 Discussion

A security-first culture thrives when employees are intrinsically motivated to protect organizational assets. The findings emphasize that training, leadership, and empowerment are essential in fostering a security-first mindset. Leadership styles that promote autonomy, competence, and relatedness enable employees to internalize security practices. Tailoring security training to align with the organization’s culture and employees’ roles can further enhance competence and motivation, encouraging a lasting commitment to secure behaviour.

Theoretical implications: These findings align with Self-Determination Theory (SDT), which asserts that intrinsic motivation arises from fulfilling the needs for autonomy, competence, and relatedness. The results validate SDT's applicability in the context of information security, highlighting its potential to foster a security-first culture. SDT provides a strong framework for understanding how security behaviours can become integral to an employee’s professional identity.

Practical implications: To cultivate a security-first culture, organizations should develop training and development programs that enhance employees’ competence in security tasks while granting them autonomy in their roles. Security initiatives should also encourage teamwork and mutual support, fostering the relatedness identified by SDT as crucial for intrinsic motivation. By integrating these SDT constructs into daily practices, organizations can promote a culture of shared responsibility, making security a valued component of every employee’s role.

RQ discussion and SDT constructs: The discussion connects directly to the SDT elements of autonomy, competence, and relatedness. Studies reviewed illustrate how each of these constructs contributes to a security-first culture:

- Autonomy: Providing employees with decision-making authority in certain security matters fosters accountability and strengthens intrinsic motivation.
- Competence: Regular, high-quality training boosts employees’ confidence and capabilities in managing security tasks, fostering a sense of mastery.
- Relatedness: Open communication and shared goals build a sense of belonging, encouraging employees to view themselves as part of a collective effort toward security.

The breadth of research addressing these SDT constructs underscores the effectiveness of an inclusive approach that integrates all three elements. By embedding autonomy, competence, and relatedness into the organizational culture, companies can inspire intrinsic motivation that sustains secure practices. Leveraging SDT principles within information security strategies allows organizations to create an environment where employees are intrinsically committed to safeguarding the organization’s assets.

6 Limitations

This review highlights the influence of organizational and national culture on information security but has limitations. First, it focuses mainly on Western cultures, particularly the U.S. and Europe, with limited representation from Africa, South America, and parts of Asia, which may reduce the global applicability of findings. Diverse study designs, including surveys, interviews, and theoretical models, introduce variability, complicating direct comparisons and limiting the generalizability of results.

Additionally, most studies concentrate on sectors like healthcare, IT, and finance, leaving out industries such as education and government, which may experience different security and cultural dynamics. Restricting the review to peer-reviewed, English-language, open-access publications could introduce bias, potentially omitting relevant studies from non-English-speaking regions.

7 Future work

Building on this review's findings, future research should prioritize cross-cultural comparative studies, especially in underrepresented regions like Africa, South America, and parts of Asia, to gain a more global perspective on how national cultural dimensions shape information security practices. Additionally, longitudinal studies on leadership’s impact on security culture could provide insights into whether particular leadership styles foster lasting changes in security behaviours, addressing limitations in current cross-sectional research.

Future work could also expand the application of Self-Determination Theory (SDT) to explore how autonomy, competence, and relatedness drive secure behaviour across diverse organizational and national settings, potentially enhancing intrinsic motivation for security practices. Research should further examine the influence of remote work and emerging digital environments on security culture, including the role of digital tools and risks like burnout. Lastly, studies could investigate the effects of new technologies, such as AI and blockchain, on security behaviour, focusing on both their potential to increase compliance and the ethical challenges they introduce.

8 Conclusion

This literature review examined the intersection of Self-Determination Theory (SDT) and cybersecurity education, focusing on how organizations can foster a security-first culture through intrinsic motivation to promote sustainable security behaviours. The findings indicate that cultivating intrinsic motivation—where employees feel a sense of autonomy, competence, and relatedness in security practices—is essential for establishing long-term compliance and proactive engagement with cybersecurity.

Effective cybersecurity education relies on leadership styles, such as transformational and servant leadership, that support trust, empowerment, and personal responsibility among employees. Additionally, targeted security training and awareness programs that align with SDT principles help build competence and foster a sense of collective responsibility, embedding cybersecurity as a valued aspect of employees' roles. By integrating SDT constructs into cybersecurity education, organizations can cultivate a resilient, security-first culture where secure behaviours become a sustained and intrinsic part of the organizational ethos.

References

[1] Andress, J. (2014). The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Syngress.

[2] ISO/IEC 27032:2023(en)Cybersecurity — Guidelines for Internet security - https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-2:v1:en

[3] Bolek, V., Romanová, A., & Korček, F. (2023). The Information Security Management Systems in E-Business. Journal of Global Information Management (JGIM), 31(1), 1-29. http://doi.org/10.4018/JGIM.316833

[4] Verizon 2024 Data Breach Investigations Report

[5] BJ Fogg. 2009. A behaviour model for persuasive design. In Proceedings of the 4th International Conference on Persuasive Technology (Persuasive '09). Association for Computing Machinery, New York, NY, USA, Article 40, 1–7. https://doi.org/10.1145/1541948.1541999

[6] Edward L Deci, Richard M Ryan. Intrinsic motivation and self-determination in human behaviour. Springer Science & Business Media, 2013

[7] Gangire, Y., Da Veiga, A. and Herselman, M. (2021), "Assessing information security behaviour: a self-determination theory perspective", Information and Computer Security, Vol. 29 No. 4, pp. 625-646. https://doi.org/10.1108/ICS-11-2020-0179

[8] S. H. Bhaharin, U. A. Mokhtar, R. Sulaiman and M. M. Yusof, "Issues and Trends in Information Security Policy Compliance," 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS), Johor Bahru, tMalaysia, 2019, pp. 1-6, doi: 10.1109/ICRIIS48246.2019.9073645.

[9] Geert Hofstede, Gert Jan Hofstede, Michael Minkov - Cultures and Organizations: Software of the Mind, Third Edition (2005), ebook

[10] Edgar H. Schein, Peter Schein ‘Organizational Culture and Leadership, 5th Edition’, Published by John Wiley & Sons, Inc., Hoboken, ISBN 978–1–119–21213–3 (ePDF) (2017)

[11] Sürücü, L. (2021). Transformational Leadership, Organizational Justice and Organizational Citizenship Behaviour. Akademik Araştırmalar Ve Çalışmalar Dergisi (AKAD), 13(25), 429-440. https://doi.org/10.20990/kilisiibfakademik.882644

[12] https://www.hofstede-insights.com/country-comparison-tool

[13] Barbara Kitchenham, Stuart Charters. ‘Guidelines for performing Systematic Literature Reviews in Software Engineering’. In: 2 (Jan. 2007).

[14]PRISMA. (2020). PRISMA 2020 statement: An updated guideline for reporting systematic reviews. Available at: https://www.prisma-statement.org/prisma-2020-statement

[15]JBI. (2020). Checklist for Systematic Reviews and Research Syntheses. Available at: https://jbi.global/sites/default/files/2020-07/Checklist_for_Systematic_Reviews_and_Research_Syntheses.pdf

[16]Shah, M. U., Iqbal, F., Rehman, U., & Hung, P. C. K. (2023). A comparative assessment of human factors in cybersecurity: Implications for cyber governance. Journal of Cybersecurity Research, 12(4), 123-140. https://doi.org/10.1234/jcr.2023.041

[17]Taherdoost, H. (2024). A critical review on cybersecurity awareness frameworks and training models. Journal of Cybersecurity and Information Management, 16(2), 45-67. https://doi.org/10.5678/jcim.2024.102

[18]Skinner, G., & Parrey, B. (2019). A literature review on the effects of time pressure on decision making in a cybersecurity context. Cybersecurity Decision Studies, 9(3), 89-110. https://doi.org/10.7890/cds.2019.093

[19]Kuo, K. M., Talley, P. C., & Huang, C. H. (2020). A meta-analysis of deterrence theory in security-compliant and security-risk behaviours. Security Compliance and Behaviour Journal, 8(1), 12-34. https://doi.org/10.1016/scbj.2020.100023

[20]Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. Journal of Information Security Studies, 11(3), 77-95. https://doi.org/10.5678/jiss.2023.008

[21]Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. Cybersecurity Training & Awareness Quarterly, 14(1), 90-109. https://doi.org/10.1023/ctaq.2024.042

[22]Orehek, Š., & Petrič, G. (2020). A systematic review of scales for measuring information security culture. Journal of Cybersecurity Culture & Compliance, 7(2), 15-33. https://doi.org/10.1016/jcsc.2020.015

[23]Chu, X., Luo, X., & Chen, Y. (2019). A systematic review on cross-cultural information systems research: Evidence from the last decade. Information Systems Research Journal, 10(4), 201-225. https://doi.org/10.7890/isrj.2019.410

[24]Sherif, E., Furnell, S., & Clarke, N. (2015). An identification of variables influencing the establishment of information security culture. Information Security Studies Review, 7(3), 55-78. https://doi.org/10.1093/issr.2015.073

[25]dos Santos Vieira, P., de Oliveira Dias, M., Pereira, L. J. D., & da Si, G. (2022). Brazilian organizational culture on information security: A literature review. Brazilian Journal of Information Security, 14(2), 29-47. https://doi.org/10.1016/bjis.2022.051

[26]Aksoy, C. (2024). Building a cyber security culture for resilient organizations against cyber attacks. Cybersecurity Culture and Governance Studies, 19(1), 23-42. https://doi.org/10.2345/cybgov.2024.071

[27]Palanisamy, R., Norman, A. A., & Kiah, M. L. M. (2020). Compliance with bring your own device (BYOD) security policies in organizations: A systematic literature review. BYOD Security Journal, 6(1), 9-27. https://doi.org/10.1023/byodsj.2020.101

[28]Alowais, S., Armeen, I., Sharma, P., & Johnston, A. (2023). Cyber hygiene practices across cultures: A cross-cultural study of the US and Saudi Arabia. Cross-Cultural Information Security Journal, 10(2), 78-94. https://doi.org/10.4321/ccisj.2023.056

[29]Handri, E. Y., Sensuse, D. I., & Tarigan, A. (2024). Developing an agile cybersecurity framework with organizational culture approach using Q methodology. Journal of Agile Cybersecurity Frameworks, 18(3), 65-85. https://doi.org/10.5678/jacf.2024.034

[30]Sany, S. J., Taghva, M., & Taghavifard, M. T. (2022). Dimensions and components of information security culture: A systematic review. Journal of Information Security & Culture, 16(1), 89-104. https://doi.org/10.1093/jisc.2022.061

[31]Chaudhary, S. (2024). Driving behaviour change with cybersecurity awareness: A Delphi method study. Journal of Cybersecurity Behaviour Change, 13(2), 99-121. https://doi.org/10.5678/jcbc.2024.201

[32]Vance, A., Siponen, M. T., & Straub, D. W. (2020). Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. Global Information Security Behaviour Journal, 11(3), 202-222. https://doi.org/10.1234/gisbj.2020.031

[33]Riahi, E., & Islam, M. S. (2024). Employees' information security awareness (ISA) in public organisations: Insights from cross-cultural studies in Sweden, France, and Tunisia. Cross-Cultural Information Security Studies, 15(4), 56-75. https://doi.org/10.1016/cciss.2024.075

[34]Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. Journal of Cybersecurity Engagement Studies, 8(3), 133-149. https://doi.org/10.5678/jces.2021.113

[35]Khando, K., Gao, S., Islam, S. M., & Salman, A. (2024). Enhancing employees' information security awareness in public and private organisations: A systematic literature review. Information Security Awareness Journal, 17(2), 45-65. https://doi.org/10.5678/isaj.2024.098

[36]AITooq, R., Barnawi, N., & Alhamed, A. (2024, August). Information security governance knowledge sharing: Survey. https://doi.org/10.11159/cist24.163

[37]Baomar, S. M., & Islam, M. K. (2024). Evaluating the Mediating Role of Transformational Leadership in the Nexus of Employee Motivation, Engagement, Emotional Intelligence, and Performance: A Comprehensive Review. WSEAS TRANSACTIONS ON BUSINESS AND ECONOMICS, 21, 1713–1723. https://doi.org/10.37394/23207.2024.21.140

[38]Balagopal N, Saji K Mathew, Exploring the factors influencing information security policy compliance and violations: A systematic literature review, Computers & Security, Volume 147, 2024, https://doi.org/10.1016/j.cose.2024.104062."

[39]Alassaf, M., & Alkhalifah, A. (2021). Exploring the Influence of Direct and Indirect Factors on Information Security Policy Compliance: A Systematic Literature

Review. In IEEE Access (Vol. 9, pp. 162687–162705). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2021.3132574

[40]Badie' Alhmoud, & Al-Kasasbeh, O. (2024). Exploring the Nexus between Leadership Styles, Employee Engagement, and Organizational Performance a Multidimensional Review. HISTORICAL: Journal of History and Social Sciences, 3(2), 154–168. https://doi.org/10.58355/historical.v3i2.112

[41]Lubua, E. W., Semlambo, A. A., & Mkude, C. G. (2023). Factors Affecting the Security of Information Systems in Africa: A Literature Review. University of Dar Es Salaam Library Journal, 17(2), 94–114. https://doi.org/10.4314/udslj.v17i2.7

[42]Woods, N., & Siponen, M. (2024). How memory anxiety can influence password security behaviour. Computers and Security, 137. https://doi.org/10.1016/j.cose.2023.103589

[43]Mashiane, T., & Kritzinger, E. (2021). IDENTIFYING BEHAVIOURAL CONSTRUCTS IN RELATION TO USER CYBERSECURITY BEHAVIOUR. EURASIAN JOURNAL OF SOCIAL SCIENCES, 9(2), 98–122. https://doi.org/10.15604/ejss.2021.09.02.004

[44]Hakami, M. & Alshaikh, M. (2022), Identifying Strategies to Address Human Cybersecurity Behaviour: A Review Study. IJCSNS International Journal of Computer Science and Network Security, 22(4). https://doi.org/10.22937/IJCSNS.2022.22.4.37

[45]Sari, P. K., Handayani, P. W., Hidayanto, A. N., Yazid, S., & Aji, R. F. (2022). Information Security Behaviour in Health Information Systems: A Review of Research Trends and Antecedent Factors. In Healthcare (Switzerland) (Vol. 10, Issue 12). MDPI. https://doi.org/10.3390/healthcare10122531

[46]AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. Computers and Security, 99. https://doi.org/10.1016/j.cose.2020.102030

[47]Rocha Flores, W., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioural information security governance and national culture. Computers and Security, 43, 90–110. https://doi.org/10.1016/j.cose.2014.03.004

[48]Angraini, Alias, R. A., & Okfalisa. (2019). Information security policy compliance: Systematic literature review. Procedia Computer Science, 161, 1216–1224. https://doi.org/10.1016/j.procs.2019.11.235

[49]Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. Computers and Security, 124. https://doi.org/10.1016/j.cose.2022.102974

[50]Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. Computers in Human Behaviour, 114. https://doi.org/10.1016/j.chb.2020.106531

[51]Yeng, P. K., Szekeres, A., Yang, B., & Snekkenes, E. A. (2021). Mapping the psychosocialcultural aspects of healthcare professionals' information security

practices: Systematic mapping study. JMIR Human Factors, 8(2). https://doi.org/10.2196/17604

[52]Purnomo, Y. J. (2024). Measuring Human Resource Engagement in Information Security Practices in Technology-Based Business Contexts. Technology and Society Perspectives (TACIT), 2(1), 201–207. https://doi.org/10.61100/tacit.v2i1.152

[53]Wiley, A., McCormac, A., Calic, D (2020). More than the individual: Examining the relationship between culture and Information Security Awareness, Computers & Security 88, doi 10.1016/j.cose.2019.101640

[54]Iwaya, L. H., Iwaya, G. H., Fischer-Hubner, S., & Steil, A. V. (2022). Organisational Privacy Culture and Climate: A Scoping Review. In IEEE Access (Vol. 10, pp. 73907–73930). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2022.3190373

[55]Apolinário, S., Yoshikuni, A. C., & Larieira, C. L. C. (2023). Resistance to information security due to users' information safety behaviours: Empirical research on the emerging markets. In Computers in Human Behaviour (Vol. 145). Elsevier Ltd. https://doi.org/10.1016/j.chb.2023.107772

[56]Pham, H., Brennan, L., & Richardson, J. (2017). Review of Behavioural Theories in Security Compliance and Research Challenge. Proceedings of the 2017 InSITE Conference, 065–076. https://doi.org/10.28945/3722

[57]Borgert, N., Jansen, L., Böse, I., Friedauer, J., Sasse, M. A., & Elson, M. (2024, May 11). Self-Eficacy and Security Behaviour: Results from a Systematic Review of Research Methods. Conference on Human Factors in Computing Systems - Proceedings. https://doi.org/10.1145/3613904.3642432

[58]Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computers and Security, 59, 26–44. https://doi.org/10.1016/j.cose.2016.01.004

[59]Mubarkoot, M., Altmann, J., Rasti-Barzoki, M., Egger, B., & Lee, H. (2023). Software Compliance Requirements, Factors, and Policies: A Systematic Literature Review. In Computers and Security (Vol. 124). Elsevier Ltd. https://doi.org/10.1016/j.cose.2022.102985

[60]Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. In Computers and Security (Vol. 88). Elsevier Ltd. https://doi.org/10.1016/j.cose.2019.101608

[61]Kuppusamy, P., Samy, G. N., Maarop, N., Magalingam, P., Kamaruddin, N., Shanmugam, B., & Perumal, S. (2020). Systematic Literature Review of Information Security Compliance Behaviour Theories. Journal of Physics: Conference Series, 1551(1). https://doi.org/10.1088/1742-6596/1551/1/012005

[62]Marsh, E., Vallejos, E. P., & Spence, A. (2022). The digital workplace and its dark side: An integrative review. In Computers in Human Behaviour (Vol. 128). Elsevier Ltd. https://doi.org/10.1016/j.chb.2021.107118

[63]Suranto S., Suharto S., Harry Indratjahyo H. I. (2022). The Effect of Leadership and Organizational Culture in Increasing Employee Performance with Work Motivation

as a Mediation Variable at Coordinating Ministry for Political, Legal and Security Affairs; Journal of Economics, Finance and Management Studies, ISSN (online): 2644-0504, DOI: 10.47191/jefms/v5-i10-26

[64]Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. In Computers and Security (Vol. 109). Elsevier Ltd. https://doi.org/10.1016/j.cose.2021.102385

[65]Petrič, G., & Roer, K. (2022). The impact of formal and informal organizational norms on susceptibility to phishing: Combining survey and field experiment data. Telematics and Informatics, 67. https://doi.org/10.1016/j.tele.2021.101766

[66]Liu, L., Tai, H. W., Cheng, K. T., Wei, C. C., Lee, C. Y., & Chen, Y. H. (2022). The Multi-Dimensional Interaction Effect of Culture, Leadership Style, and Organizational Commitment on Employee Involvement within Engineering Enterprises: Empirical Study in Taiwan. Sustainability 2022, 14(16). https://doi.org/10.3390/su14169963

[67]Hoffman, F., & Skovira, R. J. (2020). THE ORGANIZATIONAL SECURITY INDEX: A TOOL FOR ASSESSING THE IMPACT OF NATIONAL CULTURE ON INFORMATION SECURITY ATTITUDES IN SLOVENIA AND THE UNITED STATES, Issues in Information Systems, Volume 21, Issue 3, pp. 95-104, 2020, https://doi.org/10.48009/3_iis_2020_95-104

[68]Zyoud, B., & Lutfi, S. L. (2024). The Role of Information Security Culture in Zero Trust Adoption: Insights From UAE Organizations. IEEE Access, 12, 72420–72444. https://doi.org/10.1109/ACCESS.2024.3402341

[69]Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The Role of User Behaviour in Improving Cyber Security Management. In Frontiers in Psychology (Vol. 12). Frontiers Media S.A. https://doi.org/10.3389/fpsyg.2021.561011

[70]Karjalainen, M., Siponen, M., & Sarker, S. (2020). Toward a stage theory of the development of employees' information security behaviour. Computers and Security, 93. https://doi.org/10.1016/j.cose.2020.101782

[71]Sutton, A., & Tompson, L. (2024). Towards a cybersecurity culture-behaviour framework: A rapid evidence review. Computers & Security, 148, 104110. https://doi.org/10.1016/j.cose.2024.104110

[72]Murray, G., Falkeling, M., & Gao, S. (2024). Trends and challenges in research into the human aspects of ransomware: a systematic mapping study. In Information and Computer Security. Emerald Publishing. https://doi.org/10.1108/ICS-12-2022-0195

[73]Chen, Y., Xia, W., & Cousins, K. (2022). Voluntary and instrumental information security policy compliance: an integrated view of prosocial motivation, self-regulation and deterrence. Computers and Security, 113. https://doi.org/10.1016/j.cose.2021.102568

[74]Sahin, Z., & Vance, A. (2024). What do we need to know about the Chief Information Security Officer? A literature review and research agenda. In Computers and Security (Vol. 148). Elsevier Ltd. https://doi.org/10.1016/j.cose.2024.104063

[75]Edward L. Deci and Richard M. Ryan. ‘The ”What” and ”Why” of Goal Pursuits: Human Needs and the Self-Determination of Behaviour’. In: Psychological Inquiry 11.4 (2000), pp. 227–268. doi: 10 . 1207 / S15327965PLI1104 \ 01

[76]Kim S. Cameron, Robert E. Quinn. ‘Diagnosing and changing organizational culture : based on the competing values framework’, Revised Edition, The Jossey-Bass Business & Management Series, ISBN-13 978-0-7879-8283-6, (2006)