Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 3, 234-251
2026
Publisher: Learning Gate
DOI: 10.55214/2576-8484.v10i3.12340
© 2026 by the authors; licensee Learning Gate

Understanding employee cybersecurity behavior: The role of information security policies, organizational culture, and theory

Said Badreddine[1,2], Hamsa Al Ammari[3*]
[1]CIS Faculty, AAF Campus, Higher Colleges of Technology (HCT), Abu Dhabi, UAE.
[2]School of Computing, Engineering & Digital Technologies, Teesside University, Middlesbrough TS1 3B, UK.
[3]Advisor of the Chief Academic Officer, Higher Colleges of Technology (HCT), Central Services, Abu Dhabi, UAE; hsaleh@hct.ac.ae (H.A.A.).

Abstract: This study investigates employee cybersecurity behavior by examining the influence of organizational information security policies (ISPs), behavioral determinants, and dominant theoretical frameworks to address persistent human-related vulnerabilities in organizations. A systematic literature review was conducted across IEEE Xplore, SpringerLink, Emerald Insight, ResearchGate, World Scientific, and ScienceDirect. From 244 non-duplicate records, 64 peer-reviewed studies met the inclusion criteria. To extend the review, secondary analysis of the BCCC–CIC–IDS2017 dataset (n = 579) was performed using structural equation modeling. The findings indicate that cybersecurity behavior is shaped by the interaction of psychological factors (perceived threat, vulnerability, self-efficacy, motivation), social influences (peer behavior, cues to action), and organizational conditions (security culture, policy clarity, training, enforcement). Protection Motivation Theory, Theory of Planned Behavior, Health Belief Model, and General Deterrence Theory are most frequently applied. Empirical analysis confirms that peer behavior and cues to action significantly enhance cybersecurity engagement, while prior experience increases perceived severity and vulnerability and reduces perceived barriers. The study concludes that human-centric and integrative behavioral models are essential for improving cybersecurity compliance. Practical implications suggest that organizations should prioritize awareness programs, managerial support, and culturally aligned ISPs to strengthen cybersecurity resilience beyond technical controls alone.

Keywords: *Behavioral cybersecurity, Cybersecurity compliance, Organizational influence, Employee cybersecurity behavior, Information security policies (ISPs), Protection Motivation Theory, Security culture, Procedural knowledge, Motivation and perceived threat, Theoretical frameworks, Theory of Planned Behavior.*

1. Introduction

In the contemporary landscape dominated by digital transactions and prevalent internet usage, information security has emerged as a paramount concern for organizations worldwide. As cyber threats evolve in complexity and intensity, the focus has increasingly shifted towards the human elements of cybersecurity. Employees, often regarded as the first line of defense against cyber threats, play a critical role in the security posture of organizations [1].

This systematic literature review examines existing research on the influence of information security policies on employee cybersecurity behaviors, emphasizing the interplay between policy, behavior, and theory within organizational contexts.

The importance of comprehensive information security policies (ISPs) is well recognized in safeguarding organizational information assets. However, the effectiveness of these policies significantly depends on employee compliance and the resulting cybersecurity behavior. Despite the establishment of robust technical controls, the human factor remains a critical vulnerability, often exploited in

History: Received: 2 January 2026; Revised: 9 February 2026; Accepted: 12 February 2026; Published: 6 March 2026
* Correspondence: hsaleh@hct.ac.ae

cyberattacks. This review seeks to synthesize findings from various studies to understand how different aspects of information security policies influence employee behavior, which in turn affects an organization's overall security [2, 3].

Several dimensions are explored in this review: the direct impact of explicit information security policies on employee cybersecurity behavior, the role of procedural knowledge and motivation in enhancing security compliance, and the psychological and cultural factors that influence adherence to these policies. Additionally, this review addresses how organizational enforcement of security measures and educational interventions can modify and improve employee behavior concerning information security, as suggested by Humaidi and Alghazo [4].

This paper is structured to first outline the methodology used in selected studies, followed by a discussion of their findings. The final section will integrate these insights to suggest practical implications for organizations, propose recommendations for policy enhancements, and identify gaps for future research. By providing a comprehensive overview of how well-crafted information security policies translate into effective employee behaviors, this review contributes to the broader discourse on cybersecurity management within organizations.

2. Methodology

To conduct a comprehensive examination of the factors influencing employee cybersecurity behavior, a systematic literature review methodology was adopted. This rigorous approach involves a structured, detailed, and thorough method for identifying, evaluating, and synthesizing the existing body of research produced by scholars, researchers, and practitioners. The research questions addressed in this literature review are presented in the following table.

Table 1.
Research Questions and Aims.

ID	Research Question	Aim
1	What are the predominant factors influencing employee cybersecurity behavior as explored in the literature?	Identify and analyze the key factors influencing employee cybersecurity behavior.
2	How do organizational information security policies contribute to shaping employee cybersecurity behavior?	Examine the role of organizational information security policies in influencing and shaping employee cybersecurity behavior.
3	What theoretical frameworks are commonly employed to study information security policy compliance and employee behavior?	Explore the theoretical underpinnings utilized in research on information security policy compliance and employee behavior.

The review process consisted of several distinct stages, as outlined below:

1. Planning: In the initial stage, the scope and objectives of the literature review were defined, a review protocol was developed, and specific research questions were formulated to guide the entire review process. The research questions aimed to explore various aspects of employee cybersecurity behavior and the influence of organizational policies.
2. Literature Search and Selection: A comprehensive search was conducted using predefined keywords related to employee cybersecurity behavior, information security policies, and organizational influences. These keywords were applied across multiple academic databases and digital libraries to ensure a broad and relevant collection of literature. Inclusion and exclusion criteria were also applied to filter the search results, ensuring that only the most relevant and high-quality studies were retained for further analysis.
3. Data Extraction: Once the relevant articles were selected, key data were extracted from each study, focusing on methodologies, findings, theories used, and contexts of the studies. This data formed the basis for comparative and thematic analysis.
4. Analysis and Synthesis: Both quantitative and qualitative analyses were conducted to interpret and synthesize the findings from the gathered literature. This involved identifying patterns,

trends, and gaps in research and understanding how different factors influence employee behavior in the realm of cybersecurity within organizations.

5. Execution: The final stage involved compiling the insights gained into a coherent and structured narrative, addressing the initial research questions and aims of the review. This stage also involved critically assessing the synthesized data to draw conclusions and identify areas for future research.

Through this systematic approach, the review aims to provide a comprehensive understanding of the factors that shape employee cybersecurity behavior, the impact of organizational information security policies, and the theoretical frameworks employed in this area of research.

The strategy for literature searching is critical in extracting pertinent information for the review paper. This process involves several key stages: selecting appropriate databases, defining search keywords and terms, creating search strings, and executing the searches. The databases were chosen based on their extensive coverage and relevance to the field of information security and employee behavior. The databases used in this study include:

1. IEEE Xplore - https://ieeexplore.ieee.org
2. Springer Link - https://link.springer.com
3. Emerald Insight - https://www.emerald.com/insight
4. ResearchGate - https://www.researchgate.net
5. World Scientific - https://www.worldscientific.com
6. ScienceDirect - https://www.sciencedirect.com

In this research, a structured approach was adopted through the application of hierarchical inclusion and exclusion criteria to the filtering process. This commenced with a consensus among the researchers to screen each article against broad criteria that framed the scope of their systematic review.

The Inclusion Criteria Include:

1. Articles reporting on cyber threats or attacks in educational institutions.
2. Articles identifying vulnerabilities exploited in educational settings by cyber attackers.
3. Research related to organizational cybersecurity risk assessments in educational contexts.
4. Articles reporting on national case studies emphasizing cyber defence strategies in educational frameworks.

On The Other Hand, the Exclusion Criteria Include:

1. Studies not relevant to the predefined research questions.
2. Studies written in languages other than English.
3. Duplicate or repetitive studies.
4. Articles not specifically about cybersecurity in educational institutions.
5. Studies focused solely on technical developments, such as algorithms or software, without integrating educational perspectives or involvement.

This thorough screening process ensured that only the most relevant studies were included in the review, maintaining both the focus and the academic rigor of the research into cybersecurity challenges in educational institutions.

In the initial stage of the systematic review process, a total of 244 non-duplicate articles were identified from various academic databases, including IEEE Xplore, Springer Link, Emerald Insight, ResearchGate, World Scientific, and ScienceDirect. Following the application of the first stage of inclusion/exclusion criteria, which involved screening titles and abstracts, 86 articles were selected for further evaluation. Subsequently, upon thorough examination of the full-text articles, 64 were deemed relevant and met the criteria for inclusion in the review. This rigorous selection process ensured that only high-quality and pertinent articles were considered for analysis, contributing to the robustness and reliability of the systematic review findings. The distribution of references is demonstrated below:

Table 2.
Distribution of References from Databases.

Database	No. of References
IEEE Explore	15
Springer Link	8
Emerald	12
Research Gate	11
Science Direct	12
World Scientific	3
Others	3
Total	64

This structured approach ensured a comprehensive and meticulous review, enhancing the credibility and depth of the findings. The rigorous selection process, illustrated in the figure below, demonstrates the systematic methodology employed to filter and identify the most relevant literature for the review.

The search strategy utilized a combination of keywords and search strings related to "cybersecurity behavior," "information security policies," "employee compliance," "organizational influence," and "security culture." Searches were conducted with constraints on titles, keywords, publication years, types of publication, and abstracts to ensure a focused and relevant selection of literature. Although the timeframe for the publications was not specifically restricted, recent articles were prioritized to capture the latest developments and trends. The sources included peer-reviewed journal articles, dissertations, conference proceedings, and book chapters, all of which were in English. Following the search phase, the next step involved selecting papers based on predefined inclusion and exclusion criteria, meticulously chosen to address the research questions laid out in the literature review, as shown below:

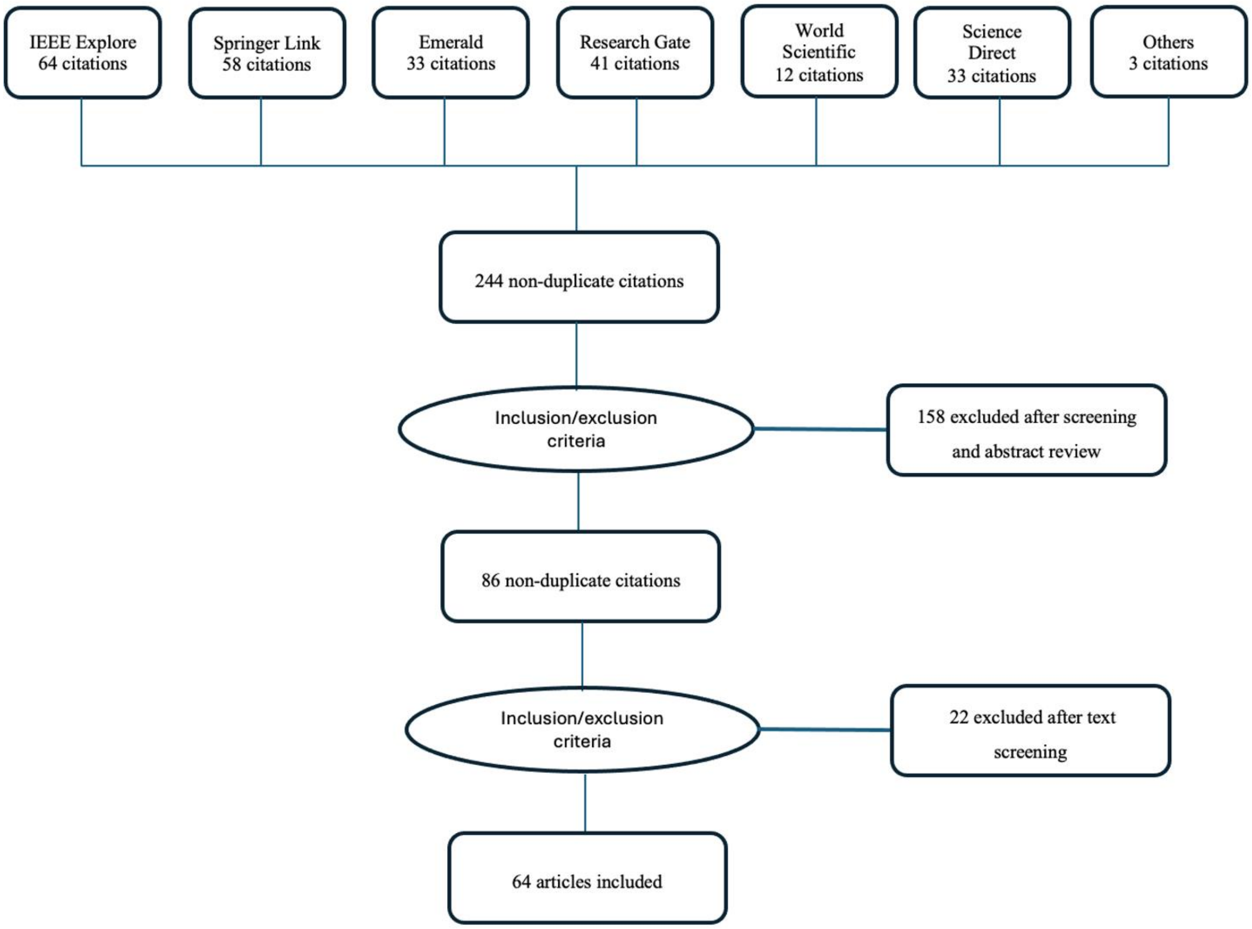

Figure 1.
Selection of Literature.

3. Conceptual Background and Model

Based on the body of available literature, we suggest a conceptual framework with three main parts (Figure 2). Peer behavior, action cues, and past information security experience are all included in the first element, which is on the left and represents the worker's commercial context. Placed in the hub, the second component focuses on how employees view information security dangers and their perceived capacity to handle them. The worker's security-conscious behavior is represented by the last element, which is on the right. Furthermore, we assess how personnel's knowledge of computer security policies affects their actions to defend against cyberattacks using this conceptual model.

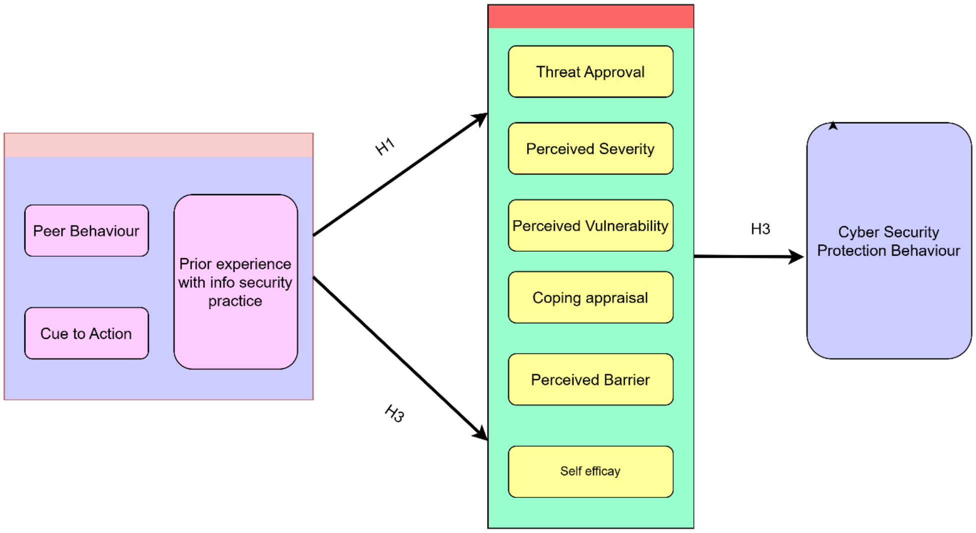

Figure 2.
Conceptual Model.

Based on the body of available literary works, we suggest a conceptual framework with three main parts (Figure 2). The initial as a result, we accept that peer conduct and cues to action are positively correlated as per Johnston and Warkentin [5] and suggest that peer behavior generates social pressure that prompts employees to respond to counter-attacks. We proposed the theory. In light of this, we suggest the following hypothesis.

- Hypothesis 1: The actions of peers have a beneficial effect on employees' prompts to engage in cybersecurity practices.

According to cybersecurity studies, staff willingness to abide by cybersecurity standards is greatly influenced by elements like peer behavior and action triggers in [6]. Workers are more likely to participate in security awareness campaigns and create anti-cybercrime strategies if they are exposed to more action triggers. Consequently, they gain greater hands-on experience in dealing with cyber threats compared to those who lack similar experiences. This practical experience proves to be an important source of knowledge, improving their capability to apply cybersecurity measures effectively in [7]. In light of this, we suggest the following hypothesis.

- Hypothesis 2: Triggers for action positively influence employees' experiences with cybersecurity measures.

The primary focus of PMT is on employees' health precautions. However, it can also be used to examine data security issues, particularly when employees require incentives to protect firm assets.
To investigate how employees assess cybersecurity threats and develop coping mechanisms from multiple perspectives, the PMT has been extensively used in [6]. The PMT relies heavily on worker activity experiences. These employee role experiences are recognized as a key component of the PMT framework. Risk assessment and coping appraisal are the two appraisal procedures that make up the PMT model. When employees experience cyberattacks, threat evaluation assesses their perceived susceptibility and level of severity.

It describes how people assess the seriousness of possible risks associated with cybersecurity attacks. It covers cases of hackers hacking into the credit card system of a bank. On the other hand, SE and response efficacy are included in coping appraisal. It concerns how people assess their capacity to control and lessen possible harm or damage resulting from a risk. This could relate to one's confidence in handling a system infected by a virus in terms of cybersecurity.

There is a perceived security risk that could cause serious harm or interruption to their workplace, according to employees. Employees typically actively seek out opportunities to learn about cybersecurity procedures or take part in company-sponsored information security training. Employees are less likely to recognize the gravity of information security threats; on the other hand, if they do not believe that they exist. As a result, employees' perceptions of the gravity of information security threats are greatly influenced by their prior security experiences, personal values, and the training they received from their companies. Employees' assessment of the risk of a cyberattack and their perception of their inadequacy in defending against it are referred to as perceived risks.

Nevertheless, employees who have prior experience handling cybersecurity incidents may feel less exposed and more equipped to avert future attacks. The organization's security management initiatives are critical in guiding employees toward taking proper security precautions and gaining essential experience for combating cyber threats. By creating an environment that promotes IT security awareness, organizations assist employees in identifying security threats and evaluating their potential consequences. Solomon and Brown [8] emphasized in their case study that the organizational atmosphere is vital in helping employees balance the exploration of new information protection techniques with adhering to existing compliance measures. Such experiences prove particularly advantageous, as employees anticipate that insights gained from security incidents will positively shape the organizational culture of compliance [8]. Ahmad's study is among the few to explore employees' cybersecurity experiences within the Protection Motivation Theory (PMT) framework. Most of the research in the PMT area in Johnston and Warkentin [5], Anderson and Agarwal [9], Herath and Rao [10], Herath and Rao [11], and Siponen et al. [12] has largely focused on the connections between threat and coping appraisals and their effect on intended behaviors. Consequently, we apply the PMT model as a holistic framework to investigate how employees' previous computer security experiences shape their perceptions of severity and vulnerability, while also evaluating the impact of PMT on shaping user behavior. This leads to the following hypothesis;

- Hypothesis 3: Workers who have greater experience in information security tend to encounter fewer challenges while carrying out cybersecurity duties.

There is no denying the magnitude of the cyber disruption. A Forbes Insights & BMC [13] poll on re-engineering information security in the age of digital transformation found that 69% of senior executives agreed that they have to review their cybersecurity policies as a result of digital transformation. Information security managers have had to deal with major organizational changes in recent years as they have implemented new procedures and technology to handle changing security risks.

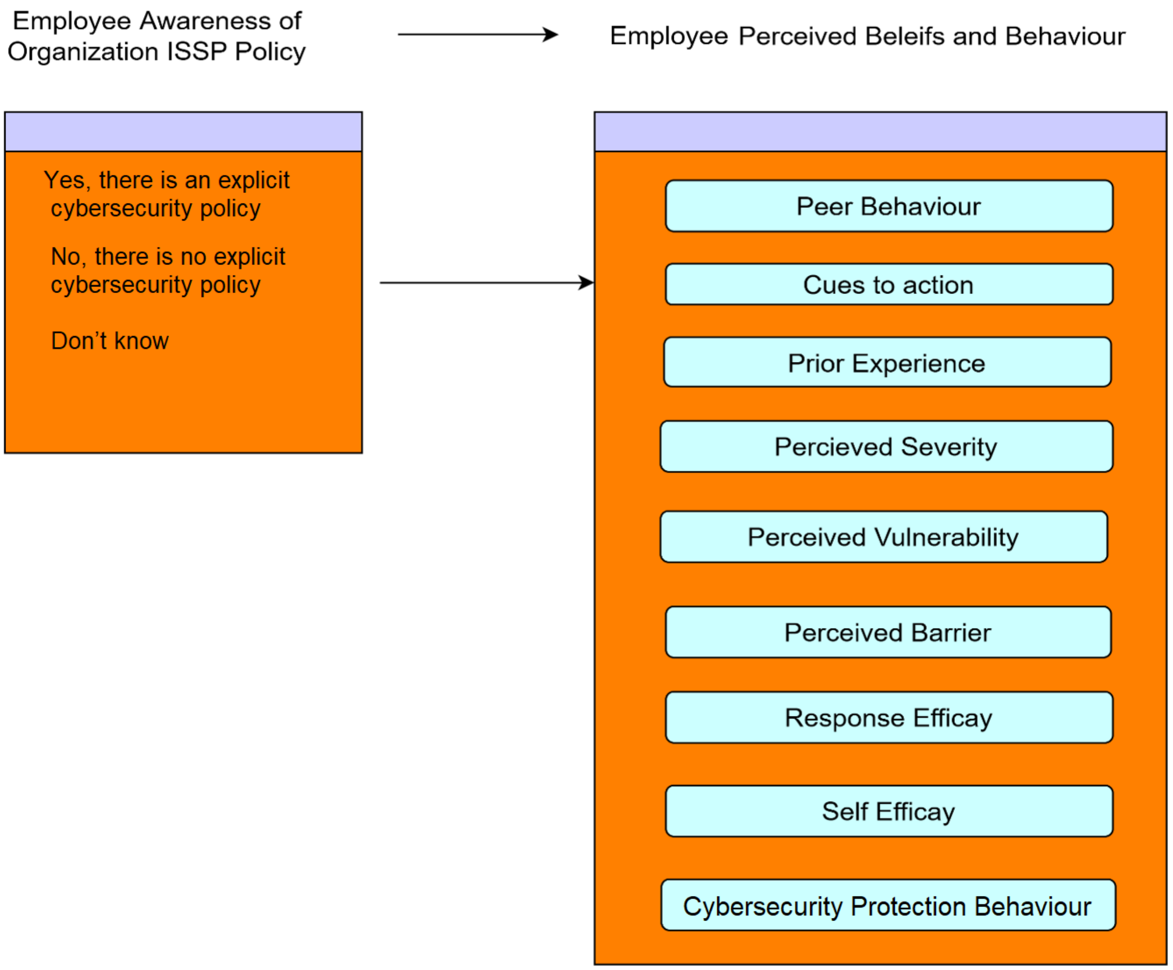
Employee Awareness of Organization ISSP Policy
Employee Perceived Beleifs and Behaviour
Yes, there is an explicit cybersecurity policy
No, there is no explicit cybersecurity policy
Don't know
Peer Behaviour
Cues to action
Prior Experience
Percieved Severity
Perceived Vulnerability
Perceived Barrier
Response Efficay
Self Efficay
Cybersecurity Protection Behaviour

Figure 3.
Cybersecurity Policy Awareness.

Even when an Information Systems Security Policy (ISSP) is in place to safeguard the organization's assets and prevent misuse, abuse, and harm to its information systems, employees often find it difficult to follow these policies. Therefore, we aim to expand our focus beyond cybersecurity behaviors to include employees' knowledge of the organization's cybersecurity policy and how that knowledge influences their actions.

According to Ifinedo [14], there are three different ways that employees feel about a company's ISSP: (i) those who know about the company's ISSP, (ii) those whose firm doesn't have one, and (iii) those who don't know if the company has one. Data from a sizable sample will be used to test the model shown in Figure 3.

4. Results and Findings

Understanding employee cybersecurity behavior is critical for developing effective security measures within organizations. Various factors, including awareness and training, organizational culture and support, motivational factors, perceived threat and self-efficacy, and policy knowledge and familiarity, influence these behaviours.

4.1. Predominant Factors Influencing Employee Cybersecurity Behavior

One of the primary influences on employee cybersecurity behaviour is awareness and training. Numerous studies highlight the importance of security education, training, and awareness (SETA) programs in enhancing cybersecurity practices among employees. For instance, Onumo [15] emphasizes that SETA programs significantly influence insiders' security-related behaviour, indicating the necessity of continuous and comprehensive training initiatives. These programs help employees understand the risks associated with cyber threats and the importance of adhering to security protocols. Chahid et al. [16] further support this view, suggesting that using multiple intervention strategies in awareness programs can effectively enhance security knowledge, attitudes, and behaviours. This finding suggests that diverse and repetitive training methods yield better results in fostering cybersecurity-conscious employee behaviour, as they address various learning styles and reinforce key security concepts over time.

Organizational culture and support also play a crucial role in shaping employee cybersecurity behaviour. Huang and Pearlson [17] highlight that a supportive organizational security culture, coupled with effective enforcement processes, positively impacts employees' attitudes towards information security compliance. This finding underscores the critical role of an organization's environment in fostering a culture of security awareness and compliance. A supportive culture encourages employees to prioritize security in their daily activities and feel confident in their ability to report suspicious activities or potential breaches. Onumo [15] further stresses the importance of aligning organizational culture with security practices, emphasizing that employees are more likely to adhere to security protocols when these practices are embedded in the organizational ethos. This alignment helps to create a unified approach to cybersecurity, where every employee understands their role in maintaining the security of the organization's information systems.

Motivational factors, both intrinsic and extrinsic, significantly influence employee cybersecurity behaviour. Chen et al. [18] employ self-determination theory (SDT) to explore these motivations, finding that autonomy, competence, and relatedness significantly influence compliance intentions. This indicates that employees are more likely to follow security policies when they feel capable, valued, and integral to the organization. Intrinsic motivation, driven by an individual's internal desires to perform a task well, plays a critical role in encouraging employees to adopt and maintain secure behaviours. Similarly, Arokodare et al. [19] discuss the balance between organizational control and individual autonomy, suggesting that clear communication and supportive policies can mitigate negative reactions and enhance compliance. This balance is essential, as overly stringent controls can lead to resistance and non-compliance, while supportive policies that respect employee autonomy can foster a cooperative and proactive security culture.

Perceived threat and self-efficacy are additional factors that shape cybersecurity behaviour. Humaidi and Alghazo [4] utilize Protection Motivation Theory (PMT) to examine how awareness of procedural security measures affects employees' cybersecurity protective behaviours. They find that increased awareness positively impacts threat appraisal and coping mechanisms, although it has a lesser effect on self-efficacy. This suggests that while employees recognize and respond to threats, they may still lack confidence in their ability to effectively manage these threats. He et al. [20] highlight the significance of security self-efficacy and prior experience, noting that these factors are particularly influential in shaping cybersecurity behaviours, with notable gender differences observed in their impact. Employees with higher self-efficacy and relevant experience are more likely to engage in proactive cybersecurity behaviours, as they feel more confident in their ability to handle security threats.

4.2. Role of Organizational Information Security Policies

Policy knowledge and familiarity also play a crucial role in influencing cybersecurity behavior. Tripathy et al. [21] and Ashraf et al. [22] demonstrate that familiarity with security policies enhances employees' ability to handle cybersecurity tasks, indicating that well-informed employees are better equipped to adhere to security protocols. This underscores the importance of disseminating clear and accessible policy information to all organizational members. Employees who understand the rationale behind security policies and procedures are more likely to comply with them, as they recognize their importance in protecting the organization's information assets.

Organizational information security policies significantly shape employee cybersecurity behavior through clarity and communication, enforcement and support, and adaptability. Clear and well-communicated policies are fundamental to effective cybersecurity practices. Li et al. [23] find that explicit information security policies significantly improve employees' cybersecurity behavior by providing clear guidelines and expectations. This clarity helps to eliminate ambiguity and ensures that employees understand their roles and responsibilities in maintaining security. Richards et al. [24] suggest that priming individuals with ethical principles can enhance their recognition of policy breaches, highlighting the importance of integrating ethical considerations into policy communication. Clear policies that are well-communicated help employees understand the importance of their actions in maintaining cybersecurity and encourage them to comply with established protocols.

Effective enforcement mechanisms and organizational support are crucial for policy compliance. AlKalbani et al. [2] indicate that organizational enforcement mechanisms positively influence employees' attitudes towards compliance, suggesting that consistent and fair enforcement practices are essential for maintaining security standards. Enforcement ensures that employees take security policies seriously and understand the consequences of non-compliance. Mohanty et al. [25] identify stress as a significant factor for cybersecurity professionals, indicating that supportive policies can mitigate stress and improve compliance. This points to the need for policies that not only set clear expectations but also provide the necessary support and resources to help employees meet these expectations. Supportive policies that address employee well-being and provide resources for managing stress can enhance compliance and overall security.

Holistic and adaptive policies are essential for addressing the dynamic nature of cybersecurity threats. Alharbi [26], Almogahed et al. [27], and Ashraf et al. [28] propose a holistic evaluation model that combines passive and active techniques to assess the effectiveness of security awareness programs. This approach suggests that policies need to be continuously evaluated and adapted to remain effective in the face of evolving cyber threats. Khaw et al. [29] and Ashraf et al. [22] developed a cybersecurity framework that identifies individual, organizational, technological, and governmental factors influencing implementation, emphasizing the need for comprehensive and adaptive policies that can respond to changing circumstances. Adaptive policies that evolve with the changing threat landscape help organizations stay ahead of potential threats and maintain robust security practices.

4.3. Theoretical Frameworks Used

Several theoretical frameworks are commonly employed to study information security policy compliance and employee behavior, including Protection Motivation Theory (PMT), Self-Determination Theory (SDT), Expectancy Theory, Organizational Control and Reactance Theories, and the Theory of Interpersonal Behavior. PMT is frequently used to understand how perceived threats and coping mechanisms influence security behaviors. Humaidi and Alghazo [4] use PMT to show that awareness of security measures positively affects threat appraisal and coping mechanisms, although self-efficacy is less impacted. This framework helps to explain how employees assess and respond to cybersecurity threats, highlighting the importance of threat perception and coping strategies in shaping behavior. SDT, employed by Alzahrani et al. [30], explores intrinsic motivations for policy compliance, focusing on autonomy, competence, and relatedness. This theory provides insights into how internal motivational factors drive employees to adhere to security policies, suggesting that fostering a sense of autonomy and competence can enhance compliance.

Burns et al. [31] utilize Expectancy Theory to assess the motivational influence of SETA programs on insiders' security behavior. This theory explains how individuals' expectations of the outcomes of their actions influence their behavior, highlighting the importance of setting clear and achievable expectations for security practices. Lowry and Moody [32] and Ashraf et al. [22] combine

Organizational Control and Reactance Theories to explain opposing motivations towards policy compliance. These theories suggest that while organizational control is necessary for ensuring compliance, it must be balanced with individual autonomy to avoid negative reactions and resistance. Wright et al. [33] use the Theory of Interpersonal Behavior to examine how interpersonal factors, such as habit and emotion, influence cybercrime preventative behaviors. This theory emphasizes the role of social and emotional factors in shaping behavior, suggesting that interpersonal relationships and emotional responses play a significant role in cybersecurity practices [2].

Alharbi [26], Almogahed et al. [27], and Ashraf et al. [28] propose a holistic evaluation model that integrates machine learning techniques to assess the effectiveness of security awareness programs. This innovative approach highlights the potential of combining advanced technologies with theoretical models to enhance the assessment and implementation of cybersecurity practices. By leveraging machine learning and other advanced technologies, organizations can gain deeper insights into employee behavior and the effectiveness of security programs, allowing for continuous improvement and adaptation to new threats [25].

In conclusion, the findings in Table 3 from the systematic review provide a detailed understanding of the factors influencing employee cybersecurity behavior, the role of organizational policies, and the theoretical frameworks used to study these issues. These insights form a holistic view of the cybersecurity landscape within organizational contexts, emphasizing the importance of awareness, culture, motivational factors, clear policies, and adaptive frameworks in enhancing cybersecurity practices.

Table 3.
Summary of Findings and Key References.

Findings	**Key References**
Awareness and Training: Crucial for understanding risks and compliance.	Burns et al. [31] and Sulaiman et al. [34]
Organizational Culture and Support: A supportive culture fosters security priorities.	Onumo [15] and AlKalbani et al. [2]
Motivational Factors: Intrinsic motivations like autonomy, competence, and relatedness.	Alzahrani et al. [30] and Lowry and Moody [32]
Perceived Threat and Self-Efficacy: Confidence in managing threats enhances proactive behaviours.	Arokodare et al. [19], Anderson and Agarwal [9], and Herath and Rao [10]
Policy Knowledge and Familiarity: Knowledgeable employees handle cybersecurity tasks better.	Solomon and Brown [8], Ashraf et al. [22], and Li et al. [23]
Clarity and Communication: Clear policies reduce ambiguity and promote compliance.	Ashraf et al. [22], Li et al. [23] and Richards et al. [24]
Enforcement and Support: Consistent enforcement and support enhance compliance.	Alharbi [26], and AlKalbani et al. [2]
Adaptability: Continuous evaluation and adaptation of policies are necessary.	Alharbi [26] and Khaw et al. [29]
Protection Motivation Theory (PMT): Explains the influence of perceived threats and coping mechanisms.	Humaidi and Alghazo [4]
Self-Determination Theory (SDT): Focuses on intrinsic motivations like autonomy and competence.	Alzahrani et al. [30]
Expectancy Theory: Assesses motivational influence of SETA programs.	Burns et al. [31]
Organizational Control and Reactance Theories: Explains the balance needed between control and autonomy.	Lowry and Moody [32]
Theory of Interpersonal Behaviour: Examines the influence of interpersonal factors on cybersecurity behaviours.	Wright et al. [33]

4.4. Extended Findings

This paper also uses the secondary dataset BCCC-CIC-IDS2017 from Kaggle to evaluate the generated hypothesis, and the dataset is publicly available and has been cited in various research studies [35]. The information contains 579 employees from a variety of U.S. firms who participated in the poll, which was created to evaluate employees' information security practices. The sociodemographic information of the respondents is summarized in Table 4. The participants' companies ranged in size from fewer than 20 to over 1,000 employees and represented various industries. Eighty-two percent of respondents were under 40. 46.11% of respondents claimed their organization had a formal cybersecurity policy, 14.68% said it did not, and 39.21% said they did not know about their company's information security policy. It is interesting to note that female employees appeared more likely than male employees to complete the online survey. Additionally, the poll showed that 65% of respondents were women and about 35% were men.

Table 4.
Socio-demographic characteristics.

	Frequency	Percent
Gender		
Male	200	34.54
Female	379	65.46
Age		
18-22	170	29.36
23-40	308	53.20
41-50	56	9.67
>50	45	7.77
Educational Background		
High level	126	7.60
Associate	119	20.55
Bachelor	140	24.18
Postgraduate	119	20.56
Others	75	12.95
Organization Category		
Government	44	7.60
Education	165	28.50
Banking and Finance	18	3.11
Information Technology	31	5.35
Retail/Warehouse	74	12.78
Real estate	43	7.45
Telecommunications	8	1.38
Healthcare/Medical	60	10.36
Military	19	3.28
Others	117	20.21
Organization Size		
1-50	209	36.10
51-500	130	22.45
>501	240	41.45
Information Security Policy		
No	85	14.68
Yes	267	46.11
Don't know	227	39.21

Further correlations between the validated constructs were calculated to assess discriminant validity (see Table 5). Every pair of constructs had correlations below the suggested cutoff of 0.90. We concluded that each of the nine constructions is unique, as none of their intercorrelations approached 1.0. Apart from perceived barriers (PB) and cybersecurity behavior (CSB), which were marginal, all constructs had average variance extracted (AVE) above the 0.5 threshold. This is because CSB is a novel concept (Table 5). The majority of the constructs meet the requirements for acceptable validity and reliability; however, a small number exhibit slightly low validity. The relationships among the validated constructs were calculated to assess discriminant validity (see Table 3). Every pair of constructs displayed correlations below the suggested cutoff point of 0.90. We concluded that each of the nine constructions is unique, as none of their intercorrelations approached 1.0. Except perceived boundaries (PB) and data security behavior (CSB), which are slightly below the 0.5 criterion since CSB is a recently introduced construct, the average variance extracted (AVE), displayed in the final column of Table 5, surpasses the 0.5 threshold for most constructs. Most constructs have acceptable validity and reliability, with a few exhibiting somewhat lower validity. As a result, our model's constructs' validity in both directions has been thoroughly proven.

Table 5.
Correlation Matrix.

	Mean	SD	PB	CA	PE	PS	PV	PB	RE	SE	ISB
Peer Behavior (PB)	4.14	1.22	1.00								
Cues to Action (CA)	3.90	1.53	0.710	1.00							
Prior Experience (PA)	4.59	1.51	0.493	0.578	1.00						
Perceived Severity (PS)	4.74	1.80	0.144	0.155	0.94	1.00					
Perceived Vulnerability (PV)	4.92	1.28	0.281	0.378	0.473	0.256	1.00				
Perceived Barriers (PB)	3.54	1.43	0.01	-0.02	-0.088	0.05	-0.110	1.00			
Response Efficacy (RE)	5.44	0.97	0.302	0.266	0.336	0.163	0.517	-0.173	1.00		
Security self-efficacy (SE)	4.13	1.68	0.201	0.219	0.327	-0.94	0.177	-0.115	0.08	1.00	
Protection Behavior (CPB)	5.57	1.11	0.200	0.176	0.263	0.04	0.308	-0.256	0.297	0.450	1.00

Note: *****Correlation is significant at the 0.01 level (2-tailed)
**Correlation is significant at the 0.05 level (2-tailed).

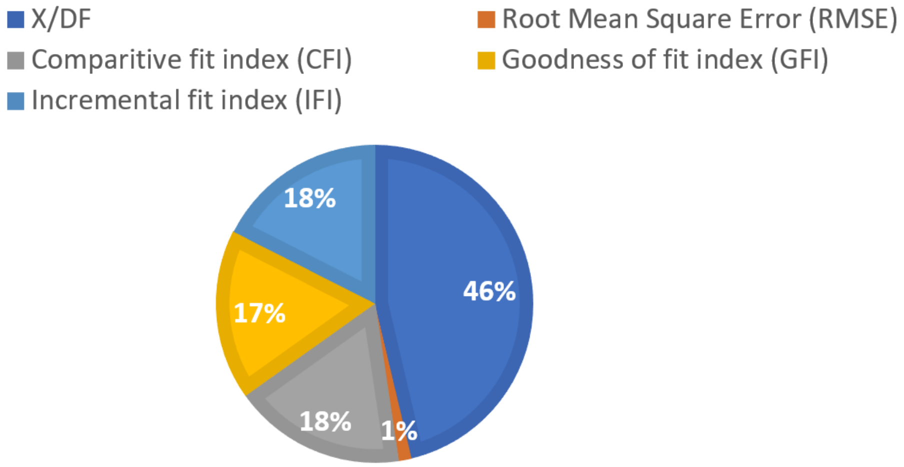

Figure 4.
FIT statistics for Measurement Model.

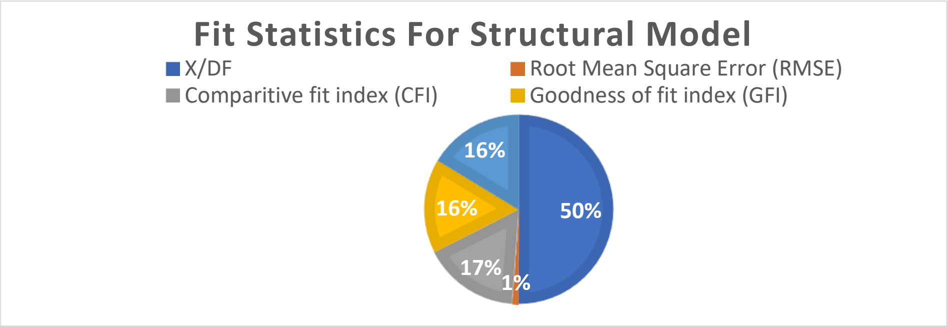

Figure 5.
F1 statistics for Structural Model.

Creating the measuring model represented in Figure 4 and assessing the structural model in Figure 5 are the two steps in the procedure. Specifically, we used the maximum likelihood approach in AMOS to evaluate the overall fit of the suggested model. Global fit measures and comparative fit measures are the two primary features reflected in the fit indices chosen for our model. The global model fit criterion is the chi-square test (χ2) with degrees of freedom. The degree to which the proposed model fits the data was evaluated using comparative fit metrics, including the comparative fit index (CFI), goodness of fit index (GFI), incremental fit index (IFI), and root mean square error of approximation (RMSEA). Usually, sample size does not affect these indices. The path parameters, which indicate the strength of the correlations among the dependent and independent variables, and the R2 values, which display the percentage of variation attributed to the independent variables, were estimated as part of the structural model test. Table 6 displays the entire set of relationships for the finished model.

Table 6.
Summary of hypothesis test results for the structural model.

Hypothesis	Paths	Standard path coefficient	p-value	Results
H1	Peer Behavior	0.53	< 0.00`	Supported
H2	Cues to action	0.74	<0.001	Supported
H3(a)	Prior Experience – Perceived severity	0.17	< 0.00`	Supported
H3(b)	Prior Experience – Perceived Vulnerability	0.62	<0.001	Supported
H3©	Prior Experience – Perceived Barriers	-0.1	< 0.00`	Supported

5. Discussion

The findings from this paper highlight significant insights into the factors influencing employee cybersecurity behavior, the role of organizational information security policies (ISPs), and the theoretical frameworks employed to study these phenomena. This discussion delves deeper into these insights, critically analyzing the implications and situating them within the broader context of existing literature.

Firstly, the predominant factors influencing employee cybersecurity behaviour, as identified in the paper, underscore the multifaceted nature of cybersecurity compliance. Psychological factors such as perceived threat severity and self-efficacy play a critical role in shaping employee actions [36, 37]. This aligns with the Protection Motivation Theory (PMT), which posits that individuals' motivation to protect themselves is influenced by their appraisal of the threat and their ability to cope with it [22, 38]. However, the review also highlights that beyond individual cognition, social and organizational influences significantly impact behaviour. For instance, the Theory of Planned Behaviour (TPB) emphasizes the role of social norms and perceived behavioural control in predicting compliance [39]. The integration of these theories suggests a comprehensive model of cybersecurity behaviour that includes individual, social, and organizational dimensions.

The role of ISPs in shaping employee behaviour is another critical area illuminated by the review. Effective ISPs are not just about delineating rules but also about fostering a security culture. This is supported by Herath et al. [40], who argue that security policies must be embedded within the organizational culture to be effective. The review findings emphasize that policies should be clear, enforceable, and supported by continuous training and awareness programs. Moreover, the importance of management support and the establishment of a positive security culture cannot be overstated. When employees perceive that their organization prioritizes cybersecurity and supports their compliance efforts, they are more likely to adhere to security policies.

The paper also sheds light on the theoretical frameworks commonly used to study information security policy compliance and employee behaviour. While PMT and TPB are frequently employed, the Health Belief Model (HBM) and the General Deterrence Theory (GDT) also offer valuable insights. HBM, with its focus on perceived benefits and barriers, can explain why employees may choose to follow or disregard security policies [22, 41, 42]. GDT, on the other hand, highlights the role of sanctions and monitoring in deterring non-compliance [34, 43]. This theoretical plurality indicates that no single theory can fully explain the complexity of cybersecurity behaviour, suggesting the need for integrative models that draw on multiple theoretical perspectives.

While the paper provides a comprehensive overview of existing research, it also highlights several gaps and areas for future research. One significant gap is the lack of longitudinal studies that track changes in employee behavior over time. Most studies are cross-sectional, providing a snapshot rather than a dynamic view of behavior. Longitudinal studies could offer insights into how behaviors evolve and the long-term impact of interventions. Additionally, there is a need for more research on the role of emerging technologies, such as artificial intelligence and machine learning, in shaping cybersecurity behavior and policy compliance. These technologies could offer new tools for monitoring and enforcing compliance, but their implications for privacy and employee autonomy must be carefully considered.

Another critical area for future research is the exploration of cultural differences in cybersecurity behavior. The review predominantly focuses on studies conducted in Western contexts, which may not be generalizable to other cultural settings. Understanding how cultural norms and values influence cybersecurity behavior is crucial for developing globally applicable policies and interventions.

By addressing the identified gaps and exploring new avenues of research, future studies can contribute to a deeper understanding of cybersecurity behavior and the development of more effective policies and interventions. This discussion emphasizes the importance of a holistic approach to cybersecurity, considering individual, organizational, and cultural factors, supported by robust theoretical frameworks and empirical evidence.

6. Conclusion and Recommendations

This paper has provided a comprehensive examination of the factors influencing employee cybersecurity behavior, the role of organizational information security policies (ISPs), and the theoretical frameworks employed to study these phenomena. The findings underscore the complexity of cybersecurity behavior, highlighting the interplay between individual psychological factors, social influences, and organizational contexts. Effective ISPs are critical in shaping positive cybersecurity behaviors, and their success is significantly enhanced by embedding them within a supportive security culture. The review also reveals the necessity for integrative theoretical models to fully capture the multifaceted nature of cybersecurity behavior. Addressing the identified research gaps and exploring new dimensions will be crucial for advancing our understanding and enhancing organizational cybersecurity practices. Therefore, it is recommended to:

1. Foster a positive security culture through consistent management support, clear communication of the importance of cybersecurity, and recognition of employees' compliance efforts.
2. Develop and implement ongoing training and awareness programs that are engaging and tailored to different roles within the organization, emphasizing both the technical and behavioural aspects of cybersecurity.
3. Employ and develop integrative models that combine insights from multiple theories such as PMT, TPB, HBM, and GDT, to provide a more holistic understanding of cybersecurity behaviour.
4. Conduct longitudinal research to track changes in employee cybersecurity behaviour over time and assess the long-term effectiveness of interventions and policies.
5. Investigate cultural differences in cybersecurity behaviour to develop policies and interventions that are effective across diverse cultural contexts.
6. Explore the role of emerging technologies like artificial intelligence and machine learning in enhancing policy compliance and monitoring, while carefully considering their implications for privacy and employee autonomy.
7. Ensure that ISPs are not only clear and comprehensive but also practically enforceable, with defined consequences for non-compliance and consistent enforcement.
8. Establish feedback mechanisms where employees can report challenges and suggest improvements to security practices, fostering a collaborative approach to cybersecurity.

9. Regularly review and update ISPs to keep pace with evolving cyber threats and changes in the organizational environment.
10. Encourage research that delves deeper into the organizational factors influencing cybersecurity behaviour, such as leadership styles, organizational structure, and interdepartmental coordination.

By implementing these recommendations, organizations can enhance their cybersecurity posture, ensuring that their policies not only exist on paper but are effectively translated into secure employee behaviors. This proactive and comprehensive approach is essential for mitigating risks associated with cyber threats in today's digital landscape.

Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Copyright:

References

[1] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, "Gender difference and employees' cybersecurity behaviors," *Computers in Human Behavior*, vol. 69, pp. 437-443, 2017. https://doi.org/10.1016/j.chb.2016.12.040

[2] A. AlKalbani, H. Deng, and B. Kam, "The influence of organizational enforcement on the attitudes of employees towards information security compliance," in *2019 10th International Conference on Information and Communication Systems (ICICS) (pp. 152-159). IEEE*, 2019.

[3] S. Badreddine *et al.*, "Predicting cybersecurity behaviours in higher education institutions: A data-driven analysis of policy, culture, and motivation in the UAE context," *Information*, vol. 17, no. 2, p. 152, 2026. https://doi.org/10.3390/info17020152

[4] N. Humaidi and S. H. A. Alghazo, "Procedural information security countermeasure awareness and cybersecurity protection motivation in enhancing employee's cybersecurity protective behaviour," in *2022 10th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-10). IEEE*, 2022.

[5] A. C. Johnston and M. Warkentin, "Fear appeals and information security behaviors: An empirical study1," *MIS quarterly*, vol. 34, no. 3, pp. 549-566, 2010. https://doi.org/10.2307/25750691

[6] A. Vance, M. Siponen, and S. Pahnila, "Motivating IS security compliance: insights from habit and protection motivation theory," *Information & Management*, vol. 49, no. 3-4, pp. 190-198, 2012. https://doi.org/10.1016/j.im.2012.04.002

[7] A. Burton-Jones and G. S. Hubona, "The mediation of external variables in the technology acceptance model," *Information & Management*, vol. 43, no. 6, pp. 706-717, 2006. https://doi.org/10.1016/j.im.2006.03.007

[8] G. Solomon and I. Brown, "The influence of organisational culture and information security culture on employee compliance behaviour," *Journal of Enterprise Information Management*, vol. 34, no. 4, pp. 1203-1228, 2021. https://doi.org/10.1108/JEIM-08-2019-0217

[9] C. L. Anderson and R. Agarwal, "Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions1," *MIS Quarterly*, vol. 34, no. 3, pp. 613-643, 2010. https://doi.org/10.2307/25750694

[10] T. Herath and H. R. Rao, "Protection motivation and deterrence: A framework for security policy compliance in organisations," *European Journal of Information Systems*, vol. 18, no. 2, pp. 106-125, 2009. https://doi.org/10.1057/ejis.2009.6

[11] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems*, vol. 47, no. 2, pp. 154-165, 2009. https://doi.org/10.1016/j.dss.2009.02.005

[12] M. Siponen, M. A. Mahmood, and S. Pahnila, "Employees' adherence to information security policies: An exploratory field study," *Information & Management*, vol. 51, no. 2, pp. 217-224, 2014. https://doi.org/10.1016/j.im.2013.08.006

[13] Forbes Insights & BMC, *Enterprises re-engineer security in the age of digital transformation*. New York, USA: Forbes, 2017.

[14] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Computers & Security*, vol. 31, no. 1, pp. 83-95, 2012. https://doi.org/10.1016/j.cose.2011.10.007

[15] A. O. Onumo, "A behavioural compliance framework for effective cybersecurity governance and practice," Doctoral Dissertation, University of Bradford, Bradford, UK, 2020.

[16] A. Chahid, S. Ahriz, K. El Guemmat, and K. Mansouri, "Digital transformation in higher education obstacle assessment and development of strategies against cybersecurity threats: The case of Moroccan universities," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 19809-19815, 2025.

[17] K. Huang and K. Pearlson, "For what technology can't fix: Building a model of organizational cybersecurity culture," 2019. https://scholarspace.manoa.hawaii.edu/handle/10125/60074

[18] R. Chen, L. Wang, B. Wang, and Y. Zhou, "Motivational climate, need satisfaction, self-determined motivation, and physical activity of students in secondary school physical education in China," *BMC Public Health*, vol. 20, no. 1, p. 1687, 2020. https://doi.org/10.1186/s12889-020-09750-x

[19] M. Arokodare, O. Asikhia, and G. Makinde, "Strategic agility and firm performance: The moderating role of organisational culture," *Business Management Dynamics*, vol. 9, no. 3, pp. 1-12, 2019.

[20] W. He *et al.*, "Improving employees' intellectual capacity for cybersecurity through evidence-based malware training," *Journal of Intellectual Capital*, vol. 21, no. 2, pp. 203-213, 2020. https://doi.org/10.1108/JIC-05-2019-0112

[21] S. Tripathy, C. L. Rao, V. Kumar, P. H. Adity, D. Kumar, and M. Jindal, "Investigating how employees' cybersecurity behaviour is affected by their knowledge of cybersecurity policy," in *2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG) (pp. 1-6). IEEE*, 2023.

[22] R. Ashraf, M. M. S. Khan, N. A. Hitam, and S. Badreddine, "Leveraging X (formerly Twitter) for digital recruitment: A case study of the luxury hospitality sector in Al Ain, UAE," *Social Sciences & Humanities Open*, vol. 12, p. 101987, 2025. https://doi.org/10.1016/j.ssaho.2025.101987

[23] L. Li, W. He, L. Xu, A. Ivan, M. Anwar, and X. Yuan, "Does explicit information security policy affect employees' cyber security behavior? A pilot study," in *2014 Enterprise Systems Conference (pp. 169-173). IEEE*, 2014.

[24] D. Richards, S. B. Nazeer Khan, P. Formosa, and S. Bankins, "The influence of ethical principles and policy awareness priming on university students' judgements about ICT code of conduct compliance," *Organizational Cybersecurity Journal: Practice, Process and People*, vol. 2, no. 2, pp. 134-161, 2022. https://doi.org/10.1108/OCJ-01-2022-0001

[25] S. N. Mohanty, T. Singh, R. Goel, S. K. Baral, and R. Kumar, "A study on building awareness in cyber security for educational system in India using interpretive structural modellings," *International Journal of System Assurance Engineering and Management*, vol. 15, no. 6, pp. 2518-2528, 2024. https://doi.org/10.1007/s13198-024-02273-3

[26] T. Alharbi, "A holistic evaluation model for information security awareness programs in work environments," in *Proceedings of the Eighth International Conference on Mobile and Secure Services (MobiSecServ 2023), IEEE, Miami, FL, USA*, 2023.

[27] A. Almogahed *et al.*, "Towards an effective refactoring taxonomy for sustainable software systems," *PLoS One*, vol. 21, no. 1, p. e0336296, 2026. https://doi.org/10.1371/journal.pone.0336296

[28] R. Ashraf *et al.*, "Leveraging LinkedIn as a digital platform for employer branding: Evidence from the UAE hotel industry," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 20, no. 4, p. 316, 2025. https://doi.org/10.3390/jtaer20040316

[29] T. Y. Khaw, A. Amran, and A. P. Teoh, "Building a thematic framework of cybersecurity: A systematic literature review approach," *Journal of Systems and Information Technology*, vol. 26, no. 2, pp. 234-256, 2024. https://doi.org/10.1108/JSIT-07-2023-0132

[30] A. Alzahrani, C. Johnson, and S. Altamimi, "Information security policy compliance: Investigating the role of intrinsic motivation towards policy compliance in the organisation," in *2018 4th International Conference on Information Management (ICIM) (pp. 125-132). IEEE*, 2018.

[31] A. Burns, T. L. Roberts, C. Posey, R. J. Bennett, and J. F. Courtney, "Assessing the role of security education, training, and awareness on insiders' security-related behavior: An expectancy theory approach," in *2015 48th Hawaii International Conference on System Sciences (pp. 3930-3940). IEEE*, 2015.

[32] P. B. Lowry and G. D. Moody, "Explaining opposing compliance motivations towards organizational information security policies," in *2013 46th Hawaii International Conference on System Sciences (pp. 2998-3007). IEEE*, 2013.

[33] T. Wright, Z. Ruhwanya, and J. Ophoff, "Using the theory of interpersonal behaviour to explain employees' cybercrime preventative behaviour during the pandemic," *Information & Computer Security*, vol. 32, no. 4, pp. 436-458, 2024. https://doi.org/10.1108/ICS-11-2023-0228

[34] N. S. Sulaiman, M. A. Fauzi, W. Wider, J. Rajadurai, S. Hussain, and S. A. Harun, "Cyber–information security compliance and violation behaviour in organisations: A systematic review," *Social Sciences*, vol. 11, no. 9, p. 386, 2022. https://doi.org/10.3390/socsci11090386

[35] J. Jose and D. V. Jose, "Deep learning algorithms for intrusion detection systems in Internet of Things using CIC-IDS 2017 dataset. ResearchGate," 2022. https://www.researchgate.net/publication/367762160

[36] S. Badreddine, A. Alazzam, A. Omari, H. Alammari, and G. Khalifa, "The use of artificial intelligence in cybersecurity," in *Proceedings of the International Conference on Computing and Information Technology (ICCIT-25), Dhaka, Bangladesh*, 2025.

[37] D. Marikyan and S. Papagiannidis, *Protection motivation theory: A review. In TheoryHub Book.* Bristol, UK: TheoryHub, 2023.

[38] R. Van Bavel, N. Rodríguez-Priego, J. Vila, and P. Briggs, "Using protection motivation theory in the design of nudges to improve online security behavior," *International Journal of Human-Computer Studies*, vol. 123, pp. 29–39, 2019.

[39] I. Ajzen and P. Schmidt, *Changing behavior using the theory of planned behavior. In The handbook of behavior change.* London, UK: Academic Press, 2020.

[40] T. C. Herath, H. S. Herath, and J. D'Arcy, "Organizational adoption of information security solutions: An integrative lens based on innovation adoption and the technology-organization-environment framework," *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, vol. 51, no. 2, pp. 12-35, 2020. https://doi.org/10.1145/3400043.3400046

[41] M. Siponen, V. Topalli, W. Soliman, and T. Vestman, "Reconsidering neutralization techniques in behavioral cybersecurity as cybersecurity hygiene discounting," *Computers & Security*, vol. 150, p. 104306, 2025. https://doi.org/10.1016/j.cose.2024.104306

[42] G. S. Khalifa *et al.*, "Employee retention in digital age: The role of organizational justice, commitment, and digital transformation in UAE," in *2025 IEEE Smart World Congress (SWC) (pp. 198-205). IEEE*, 2025.

[43] N. F. Khan, A. Yaqoob, M. S. Khan, and N. Ikram, "The cybersecurity behavioral research: A tertiary study," *Computers & Security*, vol. 120, p. 102826, 2022. https://doi.org/10.1016/j.cose.2022.102826