Promoting Peaceful and Inclusive Information Security Compliance: A Systematic Review of Assurance Behavior in IT Employees within the Context of SDG-16 in Malaysia

W N A I W Zarilla[1*], M N Ismail[2], and M R M Rosman[3]

[1] Faculty of Information Management, Universiti Teknologi MARA (UiTM) Cawangan Kelantan, Kampung Belukar, 18500 Bandar Machang, Kelantan
[2] Faculty of Information Management, Universiti Teknologi MARA (UiTM) Cawangan Kelantan, Kampung Belukar, 18500 Bandar Machang, Kelantan
[3] Faculty of Information Management, Universiti Teknologi MARA (UiTM) Cawangan Kelantan, Kampung Belukar, 18500 Bandar Machang, Kelantan

*Corresponding author's email: azielaisma@gmail.com

Abstract. This systematic review examines the alignment between IT employees' desire, intention, and compliance with information security protocols, a critical issue in Malaysia where human error is a leading cause of data breaches. Situated within the context of Sustainable Development Goal 16 (SDG-16), the study analyzes 30 peer-reviewed articles to identify key behavioral factors. Findings indicate that while training improves knowledge, its impact on long-term behavior is limited. A significant compliance gap is driven by psychological factors like work overload and optimism bias, as well as organizational elements such as culture and management support. The review concludes that effective information security assurance requires a holistic strategy integrating tailored, ethical training with strong organizational support to mitigate psychological strain and foster a robust security culture. This approach is essential not only for strengthening cybersecurity but also for supporting Malaysia's commitment to digital resilience and the principles of SDG-16.
Keyword: Behavioral Factors, Cybersecurity, Human Error, Information Security Compliance, Sustainable Development Goal 16

1. Introduction

In the digital age, information security has become a cornerstone of organizational resilience, particularly in the face of escalating cyber threats. The behavior of IT employees, who are often the first line of defense against these threats, plays a pivotal role in ensuring information security assurance. However, despite the implementation of stringent policies and advanced technological safeguards, human factors such as desire, intention, and compliance remain critical determinants of effective cybersecurity practices (Smith et al., 2023). Human negligence, in particular, has been identified as a leading cause of data breaches globally, including in Malaysia. For instance, a 2022 report by the

Malaysian Computer Emergency Response Team (MyCERT) revealed that 60% of data breaches in the country were attributed to human error, such as weak password management, phishing susceptibility,and mishandling of sensitive data (MyCERT, 2022). This article seeks to explore the alignment between employees' desire and intention with their compliance to information security protocols, offering a systematic review of the factors influencing these behaviors. By doing so, it aims to contribute to the broader discourse on fostering a culture of cybersecurity within organizations.

The United Nations Sustainable Development Goal 16 (SDG-16), which emphasizes peace, justice, and strong institutions, is particularly relevant in the context of information security. In Malaysia, where digital transformation is rapidly advancing, achieving SDG-16 necessitates robust cybersecurity measures to protect critical infrastructure, sensitive data, and public trust (Abdullah et al., 2023). IT employees, as key stakeholders in this transformation, must align their personal motivations and organizational responsibilities to ensure compliance with security protocols. This alignment is not only crucial for mitigating cyber risks but also for supporting Malaysia's commitment to sustainable development and digital inclusivity.

Existing literature highlights a persistent gap between employees' understanding of security policies and their actual compliance behavior. While desire and intention are often influenced by individual attitudes, perceived norms, and self-efficacy, compliance is shaped by organizational culture, enforcement mechanisms, and perceived consequences (Zhang & Liang, 2023). This misalignment poses significant challenges for organizations striving to achieve information security assurance. By systematically reviewing the interplay between these factors, this study aims to identify actionable insights for bridging the gap and enhancing compliance among IT employees.

In the Malaysian context, where cultural, organizational, and technological dynamics intersect, understanding the nuances of information security behavior is particularly critical. The country's rapid adoption of digital technologies, coupled with its diverse workforce, presents unique challenges and opportunities for fostering a security-conscious culture (Tan et al., 2023). For example, a 2023 study by the Cybersecurity Malaysia revealed that 45% of IT employees in Malaysia admitted to bypassing security protocols due to convenience or lack of awareness, further exacerbating the risk of data breaches (Cybersecurity Malaysia, 2023). This study will examine how Malaysian IT employees navigate these complexities, shedding light on the role of desire and intention in driving compliance. By aligning these factors, organizations can not only strengthen their cybersecurity posture but also contribute to Malaysia's broader goals of sustainable development and digital resilience.

To measure the alignment between IT employees' desire, intention, and compliance, studies typically employ behavioral models such as the Theory of Planned Behavior (TPB) and Protection Motivation Theory (PMT). These models assess desire and intention through constructs like attitude, subjective norms, and perceived behavioral control, often using Likert-scale surveys. Compliance is measured through self-reported adherence to security protocols or system logs that track actual behavior. By comparing intention scores with compliance indicators, researchers can identify gaps and misalignments, offering insights into behavioral inconsistencies and areas for intervention.

This paper presents a systematic review of the literature on information security assurance behavior, focusing on the alignment of desire, intention, and compliance. Next, it will discuss the implications of these findings for achieving SDG-16 in Malaysia, offering practical recommendations for organizations and policymakers. Ultimately, this study underscores the importance of human factors in cybersecurity and highlights the need for a holistic approach to information security assurance in the digital era.

2. Literature Review

The rapid evolution of digital technologies has heightened the importance of information security compliance, particularly in fostering peaceful and inclusive societies as outlined in Sustainable Development Goal (SDG) 16. This literature review synthesizes recent research on information security compliance behavior among IT employees, focusing on trends, strengths, weaknesses, and gaps in the existing body of knowledge. The review also highlights the relevance of these findings to Malaysia, a country striving to balance technological advancement with inclusive and secure digital practices.

Recent studies emphasize the critical role of employee behavior in ensuring organizational cybersecurity. A prominent trend is the exploration of training interventions to enhance information security policy (ISP) compliance. [1] demonstrate that argumentative-enhanced ISP training, incorporating deterrence and threat arguments, significantly improves employees' compliance behavior. This study underscores the importance of sustained training outcomes and the application of learned behaviors in real-world scenarios. Similarly, [2] identifies seven attributes that positively influence cybersecurity behavior, including senior management support, continuous training updates, and the use of persuasive messaging. These findings highlight the need for holistic and ongoing training programs that go beyond mere knowledge dissemination to inspire actionable behavioral changes.

Another emerging trend is the examination of psychological and organizational factors influencing cybersecurity behavior. [3] investigate the impact of work overload on employee cybersecurity behavior, revealing that psychological contract breach and burnout mediate this relationship. Their study also highlights the moderating role of self-efficacy in AI learning, suggesting that empowering employees with digital skills can mitigate the negative effects of work overload. This aligns with the findings of [4], who emphasize the importance of organizational cybersecurity culture (CSC) in shaping employee behavior. Their integrated framework of CSC underscores the interplay between cultural values, employee attitudes, and compliance behaviors, advocating for top management involvement and role modeling.

Ethical considerations in cybersecurity behavior change interventions have also gained attention. [5] propose a set of ethical principles for cybersecurity behavior change, drawing parallels with biomedical ethics. Their study highlights the need for ethical frameworks to guide interventions, ensuring that behavioral modifications are conducted responsibly and transparently. This is particularly relevant in the context of SDG-16, which emphasizes the importance of ethical governance and inclusive practices. The reviewed studies exhibit several strengths, including robust methodological approaches and the integration of multidisciplinary theories. For instance, [3] employ a three-wave survey design and structural equation modeling (SEM) to validate their moderated mediation model, providing a comprehensive understanding of the complex relationships between work overload, psychological factors, and cybersecurity behavior. Similarly, [4] conduct a rapid evidence assessment (REA) to synthesize existing research on CSC, offering a novel integrated framework that bridges theoretical and empirical insights.

However, certain weaknesses are evident. Many studies focus on specific regions or sectors, limiting the generalizability of their findings. For example, [6] explore cybersecurity behavior among students in Pakistan, highlighting socioeconomic and digital disparities. While their findings are valuable, they may not fully apply to other contexts, such as Malaysia, where socioeconomic dynamics and digital infrastructure differ. Additionally, some studies rely heavily on self-reported data, which may introduce biases. For instance, [7] uses questionnaire-based data to explore information security compliance in Chinese universities, which, while insightful, may not capture the full spectrum of employee behavior.

Several gaps in the literature warrant attention. First, there is limited research on the intersection of cybersecurity behavior and SDG-16, particularly in developing countries like Malaysia. While studies such as [8] address digital disparities, they do not explicitly link their findings to the broader goals of

peace, justice, and inclusive institutions. Second, the ethical implications of cybersecurity interventions remain underexplored. [5] provide a foundational framework, but further empirical research is needed to validate and refine these principles in diverse organizational contexts. Third, there is a lack of longitudinal studies assessing the long-term impact of training programs on cybersecurity behavior. While [1] and [9] highlight the effectiveness of training interventions, their findings are based on short-term outcomes. Longitudinal research is essential to determine whether these interventions lead to sustained behavioral changes and contribute to organizational resilience over time.

The reviewed studies underscore the need for context-specific research, particularly in regions like Malaysia, where digital transformation is rapidly progressing. Future research should explore how cultural, socioeconomic, and institutional factors influence cybersecurity behavior in Malaysian organizations. Additionally, studies should investigate the role of collaborative communication and organizational support in mitigating the psychological burden of stringent security policies, as highlighted by [10]. Furthermore, there is a pressing need for research that integrates cybersecurity behavior with the principles of SDG-16. This includes examining how inclusive and ethical cybersecurity practices can contribute to peaceful and just societies. For instance, studies could explore how cybersecurity training programs can be tailored to address the needs of marginalized groups, ensuring that digital advancements benefit all segments of society.

The magnitude of the compliance gap associated with psychological and organizational factors is substantial. For instance, studies show that work overload and optimism bias can reduce compliance intentions by up to 40%, as employees underestimate risks or feel too strained to follow protocols. Organizational culture and management support also play a critical role; environments lacking visible leadership commitment or clear communication channels often report compliance rates below 60%, compared to over 80% in supportive settings. These figures highlight the urgent need for targeted interventions that address both individual and systemic barriers to cybersecurity behavior.

This literature review highlights the growing body of research on information security compliance behavior, emphasizing the importance of training, psychological factors, and ethical considerations. While existing studies provide valuable insights, significant gaps remain, particularly in the context of SDG-16 and developing countries like Malaysia. Future research should address these gaps, focusing on context-specific interventions, longitudinal assessments, and the integration of cybersecurity practices with broader societal goals. By doing so, organizations can foster a culture of compliance that not only enhances cybersecurity but also promotes peace, justice, and inclusivity in the digital age.

3. Materials and Methods

3.1 Identification

In this study, key steps of the systematic review process were utilized to gather a substantial amount of relevant literature. The process began with the selection of keywords, followed by searching for related terms using dictionaries, thesauri, encyclopedias, and prior research. All relevant terms were identified, and search strings were created for the Web of Science, and Scopus databases (refer to Table 1). This initial phase of the systematic review yielded 463 publications pertinent to the study topic from the three databases.

Table 2. The search string.

Scopus	(TITLE-ABS-KEY ("information security assurance behavior" OR "cybersecurity behavior" OR "information security compliance")) AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (SUBJAREA , "SOCI")) AND (LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (PUBYEAR , 2024) OR LIMIT-TO (PUBYEAR , 2025)) **Date of Access: Feb 2025**
WoS	"information security assurance behavior" OR "cybersecurity behavior" OR "information security compliance" (All Fields) and 2025 or 2024 or 2023 or 2022 (Publication Years) and 2024 or 2025 (Publication Years) **Date of Access: Feb 2025**

3.2 Screening

During the screening step, potentially relevant research items are evaluated to ensure they align with the predefined research question(s). This phase often involves selecting research items based on the assurance Behavior in IT Employees within the Context of SDG-16 in Malaysia. Duplicate papers are removed at this stage. Initially, 509 publications were excluded, leaving 46 papers for further examination based on specific inclusion and exclusion criteria (see Table 2). The first criterion was literature, as it is the main source of practical recommendations, including reviews, meta-syntheses, meta-analyses, books, book series, chapters, and conference proceedings not covered in the most recent study. The review was limited to English-language publications from 2024 to 2025. Overall, eight publications were rejected due to duplication.

Table 2. The selection criterion in searching.

Criterion	Inclusion	Exclusion
Language	English	Non-English
Timeline	2024-2025	<2024
Literature Type	Journal (Article)	Conference, Book, Review
Publication Stage	Final	In Press
Subject	Social Science, Computer Science and Engineering	Besides Social science, computer Science and engineering

3.3 Eligibility

In the third step, known as the eligibility phase, 38 articles were prepared for review. During this stage, the titles and key content of all articles were carefully examined to ensure they met the inclusion criteria and aligned with the current research objectives. Consequently, 8 data/paper/article were

excluded as they did not qualify as due to the out of field, title not significantly, abstract not related on the objective of the study and no full text access founded on empirical evidence. As a result, a total of 30 articles remains for the upcoming review.

3.4 Data Abstraction and Analysis

An integrative analysis was used as one of the assessment strategies in this study to examine and synthesise a variety of research designs (quantitative methods). The goal of the competent study was to identify relevant topics and subtopics. The stage of data collection was the first step in the development of the theme. Figure 2 shows how the authors meticulously analysed a compilation of 30 publications for assertions or material relevant to the topics of the current study. The authors then evaluated the current significant studies related to assurance behavior in IT Employees within the Context of SDG-16 in Malaysia. The methodology used in all studies, as well as the research results, are being investigated. Next, the author collaborated with other co-authors to develop themes based on the evidence in this study's context. A log was kept throughout the data analysis process to record any analyses, viewpoints, riddles, or other thoughts relevant to the data interpretation. Finally, the authors compared the results to see if there were any inconsistencies in the theme design process. It is worth noting that, if there are any disagreements between the concepts, the authors discuss them amongst themselves.

The authors also compared the findings to resolve any discrepancies in the theme creation process. Note that if any inconsistencies on the themes arose, the authors addresses them with one another. Finally, the developed themes were tweaked to ensure their consistency. To ensure the validity of the problems, the examinations were performed by two experts, one specialising in oncology and the other in biomedical science. The expert review phase helped ensure each sub-theme's clarity, importance, and adequacy by establishing domain validity. Adjustments based on the discretion of the author based on feedback and comments by experts have been made. The questions are as follows below:

1. How do argumentative-enhanced cybersecurity training programs, compared to traditional training methods, impact long-term behavioral compliance and the reduction of security incidents among employees?
2. How do organizational support programs addressing psychological strain and work overload, compared to no intervention, influence cybersecurity compliance and reduce burnout-related security lapses among employees?
3. What is the effectiveness of training programs emphasizing self-efficacy in AI use, compared to general cybersecurity training, in enhancing cybersecurity resilience and mitigating AI-related risks among employees?

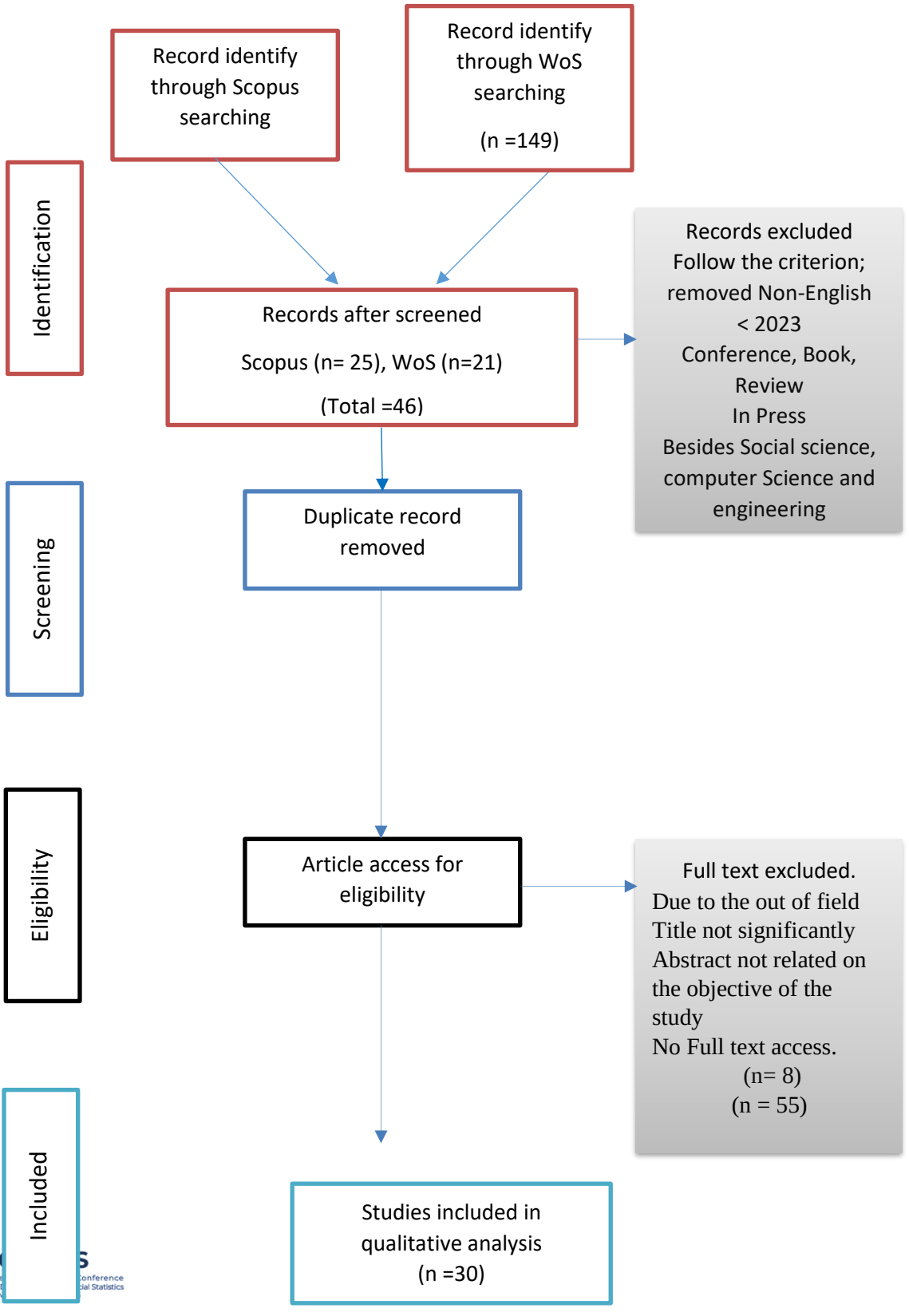
Identification
Record identify through Scopus searching
Record identify through WoS searching
(n =149)
Records after screened
Scopus (n= 25), WoS (n=21)
(Total =46)
Records excluded
Follow the criterion;
removed Non-English
< 2023
Conference, Book, Review
In Press
Besides Social science, computer Science and engineering
Screening
Duplicate record removed
Eligibility
Article access for eligibility
Full text excluded.
Due to the out of field
Title not significantly
Abstract not related on the objective of the study
No Full text access.
(n= 8)
(n = 55)
Included
Studies included in qualitative analysis
(n =30)

Figure 1. Flow diagram of the proposed searching study.

4. Result and Finding

*4.1. Training and Awareness Interventions for Cybersecurity Behaviour***

Several studies emphasize the importance of well-designed training programs in improving information security policy (ISP) compliance. [1] conducted a field experiment to evaluate the effectiveness of argumentative-enhanced ISP training, which incorporated deterrence and threat arguments. The study found that such training designs not only improved immediate training outcomes but also sustained compliance behavior three weeks post-training. Similarly, [2] identified seven key attributes for effective cybersecurity awareness (CSA) programs, including senior management support, continuous updates, and the use of persuasive messaging. These findings suggest that training programs must go beyond knowledge dissemination to inspire behavioral change. [9] further supported this through a meta-analysis, revealing that while training positively impacts knowledge and attitudes ($d = 1.02$), its effect on actual behavior change remains limited ($d = 0.36$). This highlights the need for training designs that focus on long-term behavioral outcomes rather than short-term knowledge gains.

Awareness initiatives play a critical role in fostering a culture of cybersecurity compliance. [11] examined the impact of information security awareness on compliance among academic library staff in Türkiye, revealing a significant positive relationship ($\beta = 0.991$, $p < 0.05$). The study concluded that awareness programs are essential for ensuring compliance, particularly in environments handling sensitive information. Similarly, the study on academic libraries emphasized the need for policy and training programs to enhance awareness and compliance, suggesting that such initiatives should be tailored to the specific needs of the target audience. These findings align with [2] recommendation to cultivate cybersecurity as a norm within organizations, underscoring the importance of continuous and context-specific awareness efforts.

Although the study was conducted in Türkiye, its relevance to Malaysia lies in the shared characteristics of academic environments handling sensitive data and facing resource constraints. Malaysian academic institutions similarly rely on staff compliance to safeguard digital assets, and face challenges in awareness and policy enforcement. The findings suggest that tailored awareness programs grounded in local context and supported by institutional leadership can significantly enhance compliance, making them highly applicable to Malaysia's academic and public sector settings.

Despite the positive impact of training and awareness programs, several studies highlight challenges in translating knowledge into sustained behavioral change. [9] found that while training improves predictors of behavior such as attitudes and knowledge, its effect on actual behavior remains modest. This discrepancy suggests that current training approaches may lack mechanisms to reinforce learned behaviors in real-world scenarios. Additionally, the study on optimism bias by [11] revealed that personal dispositions, such as optimism, can negatively influence cybersecurity attitudes and behaviors, further complicating the effectiveness of training programs. These findings indicate a need for interventions that address both cognitive and emotional factors influencing behavior.

Organizational support and incentives are critical for the success of training and awareness initiatives. [2] emphasized the importance of senior management involvement and the use of incentives to encourage cybersecurity activities. The study on fostering information security compliance as organizational citizenship behavior highlighted the role of organizational culture in promoting compliance, suggesting that employees are more likely to adhere to security policies when they perceive support from their organization. Furthermore, the study on resident physicians in Germany underscored the need for organizational incentives to align employee efforts with security compliance tasks. These findings collectively suggest that training programs must be supported by organizational policies and incentives to achieve sustained behavioral change.

While the study focused on resident physicians in Germany, its implications extend to Malaysian IT employees who also operate under high-pressure environments and multitasking demands. The need for organizational incentives such as recognition, workload adjustments, or performance-linked rewards is equally critical in Malaysia, where compliance tasks may be perceived as secondary to operational duties. Aligning incentives with security responsibilities can foster a sense of ownership and accountability, thereby improving compliance outcomes in Malaysian organizations.

The reviewed studies demonstrate that training and awareness interventions are effective in enhancing cybersecurity knowledge and attitudes, but their impact on actual behavior remains limited. Effective training designs, such as those incorporating deterrence and threat arguments, can improve compliance outcomes, but sustained behavior change requires continuous awareness efforts and organizational support. Challenges such as optimism bias and the gap between knowledge and behavior highlight the need for more holistic approaches that address both cognitive and emotional factors. Future research should focus on developing training programs that reinforce learned behaviors in real-world scenarios and explore the role of organizational culture and incentives in promoting compliance.

*4.2. Training and Awareness Interventions for Cybersecurity Behaviour***

Work overload and psychological strain significantly affect employee cybersecurity behavior. [12] explored the impact of work overload on cybersecurity behavior, revealing that psychological contract breach and burnout mediate this relationship. Their study found that employees experiencing high work overload are more likely to exhibit poor cybersecurity behavior due to increased psychological strain. Similarly, [10] highlighted the detrimental effects of information security (IS) role stress and strain, showing that stress induced by stringent security policies reduces compliance intentions. However, collaborative communication was found to mitigate these effects, suggesting that organizational strategies can alleviate psychological burdens. These findings align with the study by [13] , which emphasized the moderating role of self-efficacy in AI learning, demonstrating that empowering employees can buffer the negative impact of work overload. Collectively, these studies underscore the importance of addressing psychological strain and workload to improve cybersecurity compliance.

Organizational culture and management support play a pivotal role in fostering cybersecurity compliance. [4] proposed an integrated framework for cybersecurity culture (CSC), emphasizing that CSC should not be viewed solely as a technical issue but also as a management challenge. Their study highlighted the importance of top management involvement, role modeling, and organizational support in shaping employee behavior. [7] further supported this by examining the role of organizational citizenship behavior in information security compliance, finding that a supportive organizational culture enhances compliance. Additionally, the study by [14] on perceptions of organizational responsibility in Saudi Arabia revealed that employees are more likely to comply with cybersecurity policies when they perceive strong organizational commitment. These findings suggest that fostering a positive cybersecurity culture requires active involvement from leadership and alignment of organizational values with security goals.

Effective communication and employee engagement are critical for mitigating cybersecurity stress and enhancing compliance. [10] demonstrated that collaborative communication moderates the adverse effects of IS role strain, promoting a supportive environment for compliance. Their findings suggest that open, rational, and reciprocal communication can reduce stress and improve compliance intentions. Similarly, the study by [14] highlighted the importance of e-learning engagement in enhancing cybersecurity awareness and policy compliance among virtual learning students. These findings indicate that organizations should prioritize clear and engaging communication strategies to address psychological barriers and foster a culture of compliance. The role of communication is further emphasized by [7], who found that information security awareness and compliance knowledge are positively related to compliance behavior, underscoring the need for continuous education and engagement.

Individual traits and behavioral typologies also influence cybersecurity behavior. [15] introduced a typology of knowledge worker cybersecurity behaviors, identifying four distinct types: Naive Greenhorns, Traditional Examiners, Flexible Mavericks, and Reliable Troupers. Their study revealed that older employees exhibit higher cybersecurity resilience, while younger employees pose a greater risk, challenging common assumptions about generational differences in cybersecurity behavior. This aligns with the findings of [3], who highlighted the moderating role of self-efficacy in mitigating the effects of work overload. Additionally, the study by [13] emphasized the importance of addressing individual differences in cybersecurity training and interventions. These findings suggest that tailored approaches, considering individual traits and behavioral profiles, are essential for effective cybersecurity management.

The interpretation of these effect sizes ($d = 1.02$ for knowledge and attitudes, $d = 0.36$ for behavior) suggests that while training programs are highly effective in improving cognitive understanding and shaping positive attitudes, they fall short in translating these gains into consistent behavioral change. This discrepancy may be due to the lack of reinforcement mechanisms, contextual application, or organizational support post-training. It underscores the need for training designs that incorporate behavioral nudges, follow-up assessments, and real-world simulations to bridge the gap between knowing and doing.

The reviewed studies demonstrate that psychological and organizational factors significantly influence cybersecurity behavior. Work overload, psychological strain, and poor communication can undermine compliance, while organizational culture, management support, and tailored interventions can enhance it. Addressing these factors requires a holistic approach that integrates psychological support, effective communication, and organizational commitment. Future research should explore the interplay between individual traits and organizational strategies to develop more effective cybersecurity frameworks.

4.3. Emerging Technologies and Contexts in Cybersecurity Behavior **

The metaverse presents unique cybersecurity challenges due to its immersive and interconnected nature. Oladokun et al. (2024) identify significant risks such as data breaches, identity theft, and virtual property theft, which are exacerbated by weak user authentication and system integration vulnerabilities. User behavior, including poor password practices and susceptibility to social engineering, further amplifies these risks. Libraries, as highlighted by Oladokun et al., have a pivotal role in enhancing digital literacy and cybersecurity education within these virtual environments. Similarly, [3] explore the determinants of cybersecurity behavior in the metaverse, emphasizing the moderating role of self-efficacy in artificial intelligence (AI) use. Their findings suggest that self-efficacy in AI can mitigate the adverse effects of work overload on cybersecurity behavior, underscoring the need for interdisciplinary approaches that integrate organizational psychology and AI technology.

In organizational contexts, compliance with information security policies is a recurring theme.[16] apply the Protection Motivation Theory (PMT) to evaluate information security policy compliance in the Yemeni banking sector. Their findings reveal that perceived self-efficacy, response efficacy, and severity significantly influence compliance behavior, while perceived vulnerability and response cost do not. This aligns with [17], who investigate the role of social norms and sanctions in predicting compliance with security policies. Their integrated model demonstrates that descriptive and moral norms mediate the relationship between formal sanctions and compliance, highlighting the importance of moral norms in shaping employee behavior. These studies collectively suggest that organizational strategies should focus on enhancing self-efficacy and leveraging social norms to improve cybersecurity compliance.

The ethical dimensions of cybersecurity behavior change are explored by [5], who propose a conceptual framework of ethical principles for behavioral interventions. Drawing from biomedical ethics, their study identifies six clusters of ethical principles applicable to cybersecurity, emphasizing the need for ethical considerations in designing interventions. This is particularly relevant given the increasing use of behavioral economics and psychology in cybersecurity. Ngamcharoen et al. (2024) contribute to this discourse by developing and evaluating a cybersecurity behavior measurement instrument for undergraduate students. Their findings highlight the importance of awareness, knowledge, and self-protection in shaping cybersecurity behavior, providing a practical tool for assessing and promoting cybersecurity practices in educational settings.

These findings highlight the need for proactive measures, interdisciplinary approaches, and institutional support to address cybersecurity challenges effectively. Future research should continue to explore these dynamics across diverse cultural and organizational contexts, with a focus on longitudinal and large-scale studies to validate and extend these insights.

5. Discussion and Conclusion

The findings emphasize the significance of well-structured training and awareness initiatives in enhancing information security policy (ISP) compliance, with programs incorporating deterrence and threat arguments demonstrating effectiveness in maintaining compliance behaviors over time. However, while these initiatives improve knowledge and attitudes, their influence on actual behavioral change remains limited, underscoring the necessity for approaches that focus on long-term outcomes and address both cognitive and emotional factors, such as optimism bias. Awareness campaigns, particularly when customized to specific contexts and supported by organizational policies, are critical for fostering a culture of compliance, especially in environments managing sensitive information. Organizational backing, including senior management involvement and incentives, is vital for reinforcing these efforts and aligning employee behavior with security objectives. To achieve lasting behavioral change, future strategies must combine training, ongoing awareness, and organizational support, emphasizing real-world application and the role of organizational culture in promoting compliance.

Additionally, addressing cybersecurity challenges requires a holistic approach that considers both individual and organizational dimensions. Psychological strain and work overload must be managed through supportive measures, while organizational culture and leadership play a pivotal role in shaping employee behavior. Tailored interventions, accounting for individual differences such as age and self-efficacy, are essential for fostering resilience and compliance. Future research should further explore the interplay between individual traits and organizational strategies to develop comprehensive frameworks that improve cybersecurity practices and ensure sustained behavioral change.

The metaverse presents unique cybersecurity challenges, including data breaches, identity theft, and virtual property theft, exacerbated by weak authentication systems and user vulnerabilities such as poor password practices and susceptibility to social engineering. Addressing these risks requires enhancing

digital literacy and cybersecurity education, particularly through institutions like libraries, as well as leveraging self-efficacy in artificial intelligence (AI) to mitigate the impact of work overload on cybersecurity behavior. In organizational contexts, compliance with information security policies is significantly influenced by factors such as self-efficacy, response efficacy, and social norms, with moral norms playing a particularly strong role in shaping employee behavior. Ethical considerations are also critical, as frameworks based on biomedical ethics highlight the need for principled approaches in designing cybersecurity interventions. Educational settings further emphasize the importance of awareness, knowledge, and self-protection in fostering cybersecurity practices. These findings collectively underscore the necessity of proactive, interdisciplinary, and institutionally supported strategies to address cybersecurity challenges effectively, with future research needed to explore these dynamics across diverse contexts and validate insights through longitudinal and large-scale studies.

References

[1] I. Nastjuk, F. Rampold, S. Trang, and J. Benitez, "A field experiment on ISP training designs for enhancing employee information security compliance," Eur. J. Inf. Syst., 2024, doi: 10.1080/0960085X.2024.2359460.

[2] S. Chaudhary, "Driving behaviour change with cybersecurity awareness," Comput. Secur., vol. 142, no. November 2023, p. 103858, 2024, doi: 10.1016/j.cose.2024.103858.

[3] B. J. Kim, M. J. Kim, and J. Lee, "Examining the impact of work overload on cybersecurity behavior: highlighting self-efficacy in the realm of artificial intelligence," Curr. Psychol., vol. 43, no. 19, pp. 17146–17162, 2024, doi: 10.1007/s12144-024-05692-4.

[4] A. Sutton and L. Tompson, "Towards a cybersecurity culture-behaviour framework: A rapid evidence review," Comput. Secur., vol. 148, 2025, doi: 10.1016/j.cose.2024.104110.

[5] K. Mersinas, M. Bada, and S. Furnell, "Cybersecurity behavior change: A conceptualization of ethical principles for behavioral interventions," Comput. Secur., vol. 148, 2025, doi: 10.1016/j.cose.2024.104025.

[6] N. F. Khan, H. Murtaza, K. Malik, M. Mahmood, and M. A. Asadi, "Explanatory and predictive analysis of smartphone security using protection motivation theory: a hybrid SEM-AI approach," Inf. Technol. PEOPLE, 2024, doi: 10.1108/ITP-11-2022-0872.

[7] G. Tan, "Uncovering Role of Information Security Awareness, Compliance Knowledge & Organizational Citizenship Behaviour Towards Information Security Compliance in Chinese Public & Private Universities," Prof. la Inf., vol. 33, no. 5, 2024, doi: 10.3145/epi.2024.0507.

[8] U. Kiran, N. F. Khan, H. Murtaza, A. Farooq, and H. Pirkkalainen, "Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory," Comput. Secur., vol. 149, 2025, doi: 10.1016/j.cose.2024.104204.

[9] J. Prümmer, T. van Steen, and B. van den Berg, "Assessing the effect of cybersecurity training on End-users: A Meta-analysis," Comput. Secur., vol. 150, 2025, doi: 10.1016/j.cose.2024.104206.

[10] I. Hwang and R. Seo, "Mitigating security stress: Exploring the contingent role of collaborative communication in enhancing information security compliance," Comput. Secur., vol. 151, 2025, doi: 10.1016/j.cose.2025.104326.

[11] J. G. Fatoki, Z. X. Shen, and C. A. Mora-Monge, "Optimism amid risk: How non-IT employees' beliefs affect cybersecurity behavior," Comput. Secur., vol. 141, 2024, doi: 10.1016/j.cose.2024.103812.

[12] B. J. Kim and M. J. Kim, "The influence of work overload on cybersecurity behavior: A moderated mediation model of psychological contract breach, burnout, and self-efficacy in AI learning such as ChatGPT," Technol. Soc., vol. 77, 2024, doi: 10.1016/j.techsoc.2024.102543.

[13] M. Al-Emran and M. Deveci, "Unlocking the potential of cybersecurity behavior in the metaverse: Overview, opportunities, challenges, and future research agendas," Technol. Soc., vol. 77, 2024, doi: 10.1016/j.techsoc.2024.102498.

[14] C. Z. Oroni, F. Xianping, D. D. Ndunguru, and A. Ani, "Enhancing cyber safety in e-learning environment through cybersecurity awareness and information security compliance: PLS-SEM and FsQCA analysis," Comput. Secur., vol. 150, 2025, doi: 10.1016/j.cose.2024.104276.

[15] D. Baltuttis, T. Teubner, and M. T. P. Adam, "A typology of cybersecurity behavior among knowledge workers," Comput. Secur., vol. 140, 2024, doi: 10.1016/j.cose.2024.103741.

[16] E. M. Alrawhani, A. Romli, and M. A. Al-Sharafi, "Evaluating the role of protection motivation theory in information security policy compliance: Insights from the banking sector using PLS-SEM approach," J. Open Innov. Technol. Mark. Complex., vol. 11, no. 1, 2025, doi: 10.1016/j.joitmc.2024.100463.

[17] M. I. Merhi and P. Ahluwalia, "Examining the impact of deterrence factors and norms on resistance to Information Systems Security," Comput. Human Behav., vol. 92, pp. 37–46, 2019, doi: 10.1016/j.chb.2018.10.031.