University of Kent

Kent Academic Repository

Rao Faizan, Ali, Ali, Kashif, As Almerri, Khalifah, Malik, Nosheen, Alwadain, Ayed and Fati, Suliman Mohamed (2026) ***Nexus of User and Firm Factors to Promote Cybersecurity Practices and Proactive Behavior Through a Novel SEM-Machine Learning Approach.*** **Human Behavior and Emerging Technologies . ISSN 2578-1863.**

Downloaded from

https://kar.kent.ac.uk/116428/ The University of Kent's Academic Repository KAR

The version of record is available from

https://doi.org/10.1155/hbe2/2009721

This document version

Publisher pdf

DOI for this version

Licence for this version

CC BY (Attribution)

Additional information

Versions of research works

Versions of Record

If this version is the version of record, it is the same as the published version available on the publisher's web site. Cite as the published version.

Author Accepted Manuscripts

If this document is identified as the Author Accepted Manuscript it is the version after peer review but before type setting, copy editing or publisher branding. Cite as Surname, Initial. (Year) 'Title of article'. To be published in ***Title of Journal*** , Volume and issue numbers [peer-reviewed accepted version]. Available at: DOI or URL (Accessed: date).

Enquiries

If you have questions about this document contact ResearchSupport@kent.ac.uk. Please include the URL of the record in KAR. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies).

Check for updates

Human Behavior and Emerging Technologies

WILEY

RESEARCH ARTICLE OPEN ACCESS

Nexus of User and Firm Factors to Promote Cybersecurity Practices and Proactive Behavior Through a Novel SEM-Machine Learning Approach

Rao Faizan Ali[1] | Kashif Ali[2] | Khalifah As Almerri[3] | Nosheen Malik[4] | Ayed Alwadain[5] | Suliman Mohamed Fati[6]

[1]School of Computing, University of Kent, Canterbury, Kent, UK | [2]UCP Business School, Faculty of Management Sciences, University of Central Punjab, Lahore, Punjab, Pakistan | [3]Azman Hashim International Business School, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia | [4]Department of Education, The Islamia University of Bahawalpur, Bahawalpur, Punjab, Pakistan | [5]Computer Science Department, Community College, King Saud University, Riyadh, Saudi Arabia | [6]Information Systems Department, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia

Correspondence: Rao Faizan Ali (r.f.ali@kent.ac.uk)

Received: 28 October 2025 | **Revised:** 4 July 2026 | **Accepted:** 16 September 2026

Academic Editor: Maheswaran S

Keywords: cybersecurity | Industry 5.0 | machine learning | proactive behavior | STS theory

ABSTRACT

In Industry 5.0 (I5.0), cybersecurity is a strategic priority for manufacturing firms. In the I5.0 context, human–machine collaboration requires proactive employee behavior to anticipate and mitigate cyber threats. However, existing literature largely examines user or technical factors in isolation and overlooks the joint optimization of social and technical factors. To address these, this study investigates the user-level social and firm-level technical factors to explain the cybersecurity awareness, compliance, and employee proactive behavior in the I5.0 context. Based on the socio-technical systems (STS) theory, a concept framework has been developed. A survey-based quantitative method was applied to collect data from 198 employees working in Malaysian manufacturing enterprises. A dual-stage analytical technique was used, combining partial least squares structural equation modeling (PLS-SEM) with machine learning (ML). The originality of this technique stems from the combination of PLS-SEM explanatory power with ML prediction capabilities. The PLS-SEM findings affirmed that both user-level social factors and firm-level technical factors positively drive cybersecurity compliance. Surprisingly, the relationship between cybersecurity awareness and compliance was positive but insignificant. ML outcomes highlight that user and firm factors predict (85.79%) employee proactive behavior. It reinforces the robustness and predictive capability of the integrated framework. This study provides a novel explanation of social and technical factors to employee proactive behavior through cybersecurity awareness and compliance in I5.0. The study findings provide both theoretical contributions, particularly in the advancement of STS theory, as well as practical implications for managers and policymakers seeking to improve cybersecurity frameworks.

1 | Introduction

In an ever-changing digital landscape, the notion of cybersecurity has emerged as a paramount organizational priority, especially in Industry 5.0 (I5.0). In the I5.0 context, the human–machine collaboration is the cornerstone for value creation. According to Czeczot et al. [1], I5.0 refers to a new level of seamless and harmonious integration between people, machines, and automation. Unlike previous industrial revolutions like I4.0, I5.0 introduces a paradigm shift from human-centric, resilience, and sustainability [2, 3]. Moreover, I4.0 is driven by a technology-push approach, whereas I5.0 emphasizes the interaction of

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

Copyright © 2026 Rao Faizan Ali et al. *Human Behavior and Emerging Technologies* published by John Wiley & Sons Ltd.

humans with advanced technologies like artificial intelligence, robotics, and big data [4]. Consequently, the increased reliance on advanced technologies intensifies cybersecurity vulnerabilities and highlights human behavior as a critical component of organizational security framework [4, 5]. Therefore, the cybersecurity concept is no longer solely a technical concern but a social and technical challenge that requires proactive employee behavior to anticipate and mitigate cyber threats.

At the global level, the severity of cybersecurity incidents further underscores the urgency of addressing this issue. According to the Statista [6] report, more than half of firms face cyber incidents and incur losses amounting to $300 thousand. Likewise, IBM [7] reports highlight that the global average cost of cyber breaches reached $4.88 million. The cyber incidents of Saudi Aramco and Scandinavian Airlines highlight the severity and disruptive nature of these threats [8, 9]. Apart from the financial damages, cybersecurity incidents threaten firm data integrity, reputation, and even human safety [10]. More precisely, Malaysian manufacturing firms are swiftly adopting advanced technologies (AI and IoT); resultantly, it significantly expands its cyberattack extent (Manpower [11]). According to the Industrial Cyber [12] report, Malaysian manufacturing firms experience a sharp rise in cyber incidents. From a socio-technical perspective, organizations tackle this problem through technical systems and overlook the social/user aspects. This mismatch makes manufacturing firms vulnerable to transforming cybersecurity awareness (CA) into cybersecurity compliance (CC) and proactive behavior.

The past literature has made significant contributions to understand cybersecurity at employee and firm levels [13, 14]. However, the outcomes of past studies remain fragmented. Past literature predominantly examines social/user factors [15–17] or technical factors like infrastructure and security systems [10, 18]. This dichotomous approach overlooks the joint optimization of user (social) and firm (technical) factors, which is critical in I5.0 context though human–machine dimension. Consequently, past studies lack an integrated framework of how both social and technical factors jointly promote CA, CC, and ultimately employee proactive behavior (EPB). Additionally, there are nuanced empirical evidences of cybersecurity from a sociotechnical perspective in I5.0, especially in emerging manufacturing context [18–20]. To fill these voids, the aim of this study is to examine the impact of user-level social and firm-level technical factors on CA and CC, in order to achieve higher employee proactive outcomes.

This study offers several important contributions. First, it contributes to the cybersecurity literature by integrating user (social) and firm (technical) factors into a single framework, addressing the persistent fragmentation in past studies. Second, this study contributes to the body of knowledge by advancing socio-technical systems (STS) theory application in cybersecurity domain in the I5.0 context. In doing so, the study refines STS theory by highlighting its relevance in explaining cybersecurity practices as integrated user and technical systems in I5.0 context. The methodological novelty of this study is particularly crucial for cybersecurity research. Past studies generally relied on explanatory approaches which are useful for theory testing. However, limited evidence regarding whether the exogenous factors predict proactive cybersecurity behavior in practice. Thus, this study advances prior cybersecurity research by adopting a complementary SEM-ML approach. In a nutshell, these contributions offer valuable theoretical and practical insights to strengthen cybersecurity practices in highly complex digital environment.

The remainder of the document is organized as follows. The next section illustrates the theoretical background of the research essential to contextualize the study, which leads to the development of hypotheses. Then, the research methodology section is presented. Subsequently, the analysis and results section highlights the empirical work on the collected data. Finally, the discussion and conclusion section is presented, which also includes the research contributions and limitations.

2 | Theoretical Framework and Hypotheses Development

2.1 | Theoretical Background

In the current study, STS theory provides the theoretical base. The STS theory explains the interdependence and joint optimization of user (social) and firm (technical) subsystems within organization [21]. The fundamental tenets of STS theory highlight that organizational outcomes are determined by the joint optimization of human behavior, processes, and technological infrastructures [19]. In the context of cybersecurity, the user factors (password security [PS] and browser security [BS]), CA, and CC represent the social aspects of STS theory [22]. Firm-level factors (information security policy [ISP] and management security practices [MSP]) are the technical aspects of STS theory [23]. Thus, the effectiveness of cybersecurity depends on how well these subsystems interact and reinforce each other. Sadok et al. [24] claimed that focusing on technological cybersecurity solutions has limited capacity to address the challenges, whereas the STS approach has the potential to be a more effective means of addressing the challenges of detecting and reacting to insider attacks. Zhang et al. [25] argued that STS is an essential aspect of theorizing the delivery of Chinese e-government cybersecurity services. Kim et al. [26] affirmed that STS helps firms to build and address software-related policy issues in Korea. Bishop et al. [27] argued that employee CA is shaped by multiple human and firm factors. Likewise, Badi and Nasaj [13] claimed that cybersecurity effectiveness depends on regulatory compliance, organizational systems, employee capability, and third-party relationships.

In the I5.0 context, the relevance of STS theory becomes more pronounced. Unlike prior industrial revolutions, I5.0 emphasizes human-centric, where human factors actively interact with intelligent systems (AI, IoT, and robotics) [4]. Ali [28] argued that I5.0 emphasized the integration of STS theory, where the interaction between humans and machines is central to its development [2]. This increased interaction creates dynamic socio-technical subsystems in which cybersecurity risks are constantly shaped by human actions and technological configurations [18].

The prior literature highlights that conventional cybersecurity studies generally focus on technical or technology elements, and largely ignore the interplay between user and technology factors [26]. Therefore, there is a need for a comprehensive framework

hbet, 2026, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/hbe2/2009721 by Rao Faizan Ali - University Of Texas Md Anderson Cancer Center , Wiley Online Library on [25/09/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

that should explore the interaction between user and technology factors [29]. However, the past cybersecurity literature is blurred in the context of I5.0 and requires further research [18, 19, 30]. Furthermore, Schlatt et al., [30] claimed that the majority of the cybersecurity studies solely focus on technical or user aspects. Moreover, Schlatt et al. [30] suggest that a holistic framework is essential that consists of both socio and technical factors to study the cybersecurity challenges, especially in I5.0. Thus, the current study is based on STS theory. Importantly, STS theory should not be considered just as a categorization lens for dividing social and technological aspects. Rather, its primary theoretical significance is in understanding how these subsystems coincide, interconnected, and jointly optimized to achieve organizational outcomes. Employee knowledge, password behavior, browser practices, rules, managerial routines, and compliance procedures must jointly form a cohesive system in cybersecurity. Consequently, CC and proactive behavior are determined not by knowledge or regulations alone, but by the degree to which employee cognition, organizational norms, management enforcement, and digital responsibility practices are successfully paired.

2.2 | Hypotheses Development

2.2.1 | Relationship Between Firm Factors and Cybersecurity Practices

Based on the STS theory, the firm-level dimensions (ISP and MSP) fall under the technical aspects. The concept of ISP refers to the set of policies and procedures for the responsible utilization of information security resources underneath an organization [31], whereas MSP refer to the manager's ability to adapt and reconfigure new technology to align the specific social and organizational dynamics [31]. In I5.0, the cybersecurity concept has been viewed as a firm capability to safeguard the human–machine collaboration while sustaining resilient operations under growing digital interdependence [4]. From this perspective, ISP can be viewed as a formal technical mechanism through which organizations communicate security behavior, clarify responsibilities, and institutionalize secure routines [32]. In the same vein, MSP highlights the management ability to prioritize security, allocate resources, and embed cybersecurity into daily operations [4, 31, 32]. The human-centric aspects of I5.0 highlight that clear and adaptive cybersecurity practices and policies can reduce ambiguity for employees who interact with intelligent machines [4, 32].

In past studies, both dimensions have been examined in various contexts. For instance, Ali et al. [33] examined the ISP as an organizational governance factor to promote social bound theory aspects. Hwang et al. [34] examined the association between ISP and information security awareness among Korean manufacturing firms. Asfahani [35] examined the role of human resource managers in information security awareness in Saudi Arabia. Likewise, Chaudhary [36] affirmed that management played a vital role in driving behavior change with CA. Wong et al. [37] contended that management reactive behavior helps to promote employees' CC attitude among Malaysian manufacturing SMEs. Conclusively, ISP and MSP have been examined from various perspectives; there is nuanced evidence in the human-centric perspective of I5.0. To fill this void, the following hypotheses have been proposed.

Hypothesis 1. a,b: ISP has a positive relationship with CA and CC.

Hypothesis 2. a,b: MSP has a positive relationship with CA and CC.

2.2.2 | Relationship Between User Factors and Cybersecurity Practices

Based on the STS theory, user-related factors like PS and BS represent the social subsystem. The STS theory emphasizes that system effectiveness is not solely dependent on technical aspects. It depends on how humans effectively interact with systems in practices [30]. In the cybersecurity context, employee routine activities like practicing safe browsing and two-step password verification directly impact the effectiveness of firm security mechanisms [22, 23]. These behavioral practices highlight human agency aspects within STS theory, where secure actions reinforce system integrity, whereas inattentive practices can introduce vulnerabilities despite robust technical safeguards [24]. In I5.0, the individual role becomes more significant due to human-centric nature of production systems [4]. The human-centric aspects of I5.0 shift the responsibility toward humans, requiring them to adopt secure behavioral practices to ensure system resilience and continuity [2]. From this perspective, both user-related practices can be viewed as behavioral mechanisms that promote CA and CC.

In the past literature, both user-related dimensions have been well studied in various contexts. Bang et al. [38] argued that more than 80% of users maintained their current passwords, 16% reused passwords from other websites, and 4% created new ones. In the event of a data breach, password repetition becomes highly consequential since users might not change their passwords on several sites, leaving numerous accounts open to attack [15], whereas Alqahtani [39] highlighted that more than 38% of respondents agree that installing extensions from third-party websites must be avoided to minimize the cybersecurity threats. Moreover, Alqahtani [39] argued that a good level of CA and CC with standards helps to mitigate the cyberattacks. In a nutshell, the past literature highlights PS and BS from human perspective; there is nuanced empirical work from human-centric aspect of I5.0. Thus, the following hypotheses have been proposed.

Hypothesis 3. a,b: PS has a positive relationship with CA and CC.

Hypothesis 4. a,b: BS has a positive relationship with CA and CC.

2.2.3 | Relationship Between CA and CC

Based on the STS theory, the association between CA and CC are primarily grounded in the social subsystems. This subsystem highlights human cognition, behavior and

hbet, 2026, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/hbe2/2009721 by Rao Faizan Ali - University Of Texas Md Anderson Cancer Center , Wiley Online Library on [25/09/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

decision-making processes [18]. STS theory posits that social subsystems determine that the technical subsystems are effectively enacted [24]. In the cybersecurity perspective, employee awareness highlights the understanding of threats, risks, and policy procedures [4]. CC refers the behavioral execution of employee awareness [22, 27, 40]. However, STS theory posited that awareness does not automatically translate into compliance because it depends on individual priorities and interpretation [30]. In I5.0 context, the association is complex due to human-centric and resilience nature [35, 41]. The human-centric approach of I5.0 argued that employees must understand and internalize cybersecurity into their daily practices [36]. Concurrently, the resilience aspect of I5.0 emphasizes the consistent compliance to maintain stability and continuity in highly interconnected environment [42].

Prior literature highlights CA helps to promote CC. Organizations that adhere to legal frameworks and best practices intended to reduce cyber threats are deemed to comply [43]. Potential vulnerabilities are less likely to occur when staff members and systems follow these standards regularly. Compliance also requires periodic security audits, upgrades, and assessments, which aid in spotting potential flaws and strengthening defenses [44]. Organizations that adhere to compliance standards strengthen security measures, lower the likelihood of security breaches, and promote a cybersecurity-aware culture [18]. This proactive strategy ensures that cybersecurity measures are successfully introduced and maintained over time, strengthening the system's overall resilience [35, 36, 41, 42].

Hypothesis 5. CA has a positive association with CC.

2.2.4 | Relationship Between Cybersecurity Practices and EPB

The STS theory provides the theoretical support between cybersecurity practices (awareness and compliance) and EPB. Under the lens of STS, EPB emerges from the joint optimization of social and technical subsystems [29]. The CA reflects the employee understanding, knowledge, and cognitive readiness toward cyber risks [23], whereas CC highlights that how employee behavior align with firm policies, procedures, and security protocols. Therefore, proactive behavior can be view as an advanced outcome of STS, where employee actively anticipate and respond to cyberattacks rather than merely following stated rules and regulations [4, 22]. The human-centric and resilience aspects of I5.0 contextualize the relationship. From human-centric perspective, as the employee is more aware toward cyberattacks, consequently, they take necessary steps to mitigate them [18, 35, 41], whereas the resilience aspects highlight that consistent compliance with cybersecurity enables firms to maintain stability and quickly respond in disruptions [2, 4]. Based on the above arguments, the following hypotheses have been proposed. Figure 1 shows the research framework.

Hypothesis 6. CA has a positive association with EPB.

Hypothesis 7. CC has a positive association with EPB.

2.3 | Research Methodology

The present research is grounded on the positivist research philosophy, acknowledging that the research is based on true reality and that knowledge is measurable [45]. Based on the positivism philosophy, a deductive research approach is adopted. Furthermore, a quantitative research design is adopted through a questionnaire survey strategy. The unit of analysis is the individuals working in Malaysian manufacturing firms. To reach the respondents a nonprobability sampling technique like convenience sampling is adopted. The nature of the study setting also supported the use of convenience sampling. Manufacturing firms often view cybersecurity-related data as confidential because it relates to internal regulations, employee behavior, and organizational risk exposure [46, 47]. As a result, it was not possible to get a comprehensive list of qualified employees from Malaysian manufacturing firms. Respondents were selected based on their accessibility, familiarity with firm cybersecurity practices, and voluntary participation. Nevertheless, this technique may reduce representativeness and introduce selection bias; so, the findings should be considered as evidence from readily available Malaysian manufacturing employees rather than statistically representative of the overall population. Moreover, both face-to-face and online mediums have been used to reach the study population. Before the survey, professionals in

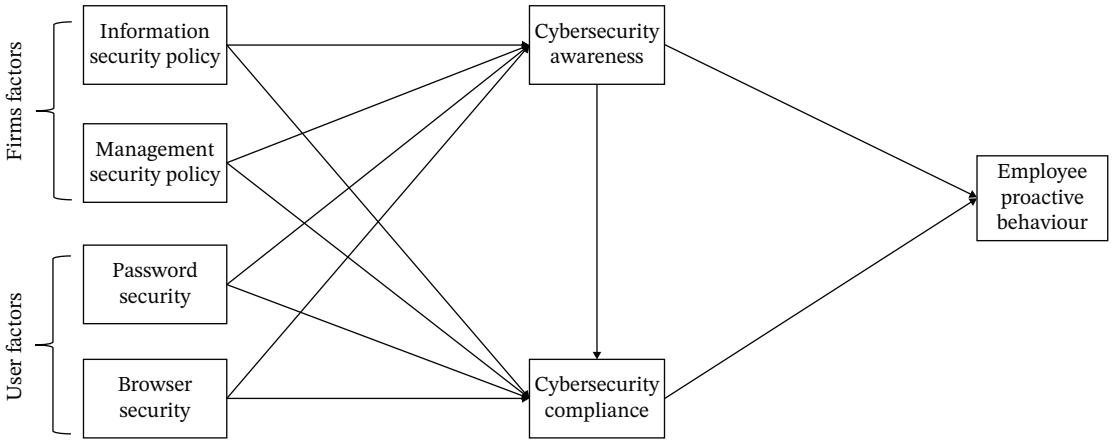


FIGURE 1 | Research framework.

hbet, 2026, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/hbe2/2009721 by Rao Faizan Ali - University Of Texas Md Anderson Cancer Center , Wiley Online Library on [25/09/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

the fields of business and academia pretested the questionnaire. Pretesting involved steps for both face and content credibility. A pilot study was carried out, and all constructs achieved the minimal threshold values while ensuring ethical principles were maintained during the data collection procedure.

The minimum sample size (146) of the study population was calculated through G*Power software [48]. In the actual survey, more than 500 questionnaires were distributed. Through follow-up emails and visits, 207 responses were received. After performing the data cleaning steps, 198 final observations were retained for advance analysis with a final response rate of 39.60%. Ali et al. [49] claimed that the average response rate of face-to-face and online techniques was fall less than 40%. Based on the prior studies' recommendations, the collected data was analyzed through the "partial least squares structural equation modeling" (PLS-SEM) technique. The partial least squares structural equation modeling (PLS-SEM) approach explains the linear assumptions and explanatory analysis [50]. PLS-SEM primarily explains the association between exogenous and endogenous variables. However, it does not fully indicate how accurately the proposed exogenous predict or classify the endogenous variables. Thus, the machine learning (ML) technique is employed as a complementary predictive validation technique. The justification of both approaches is that PLS-SEM is suitable to explain the theory-driven hypotheses, whereas ML approach is added to assess the predictive capability and robustness of the proposed framework. Moreover, the application of both approaches are consistent with past studies to generate both explanatory and predictive insights [47, 51]. The ML technique has been employed through WEKA software (Version 3.8.6). It is widely used and provides tools for data processing, classification, model comparison, statistical evaluation, and visualization. Finally, the demographic profile of the respondents is depicted in Table 1. Furthermore, Figure 2 depicts the flow of research methodology.

TABLE 1 | Demographic analysis.

Items	Type	No. of participants	Valid percent
Gender	Female	93	46.97%
	Male	105	53.03%
Age	18–25	55	27.78%
	26–35	67	33.84%
	36–50	47	23.74%
	51 or above	29	14.65%
Education	Diploma	31	15.66%
	Bachelor	138	69.70%
	Postgraduate	29	14.65%
Position	Managerial	111	56.06%
	Nonmanagerial	87	43.94%

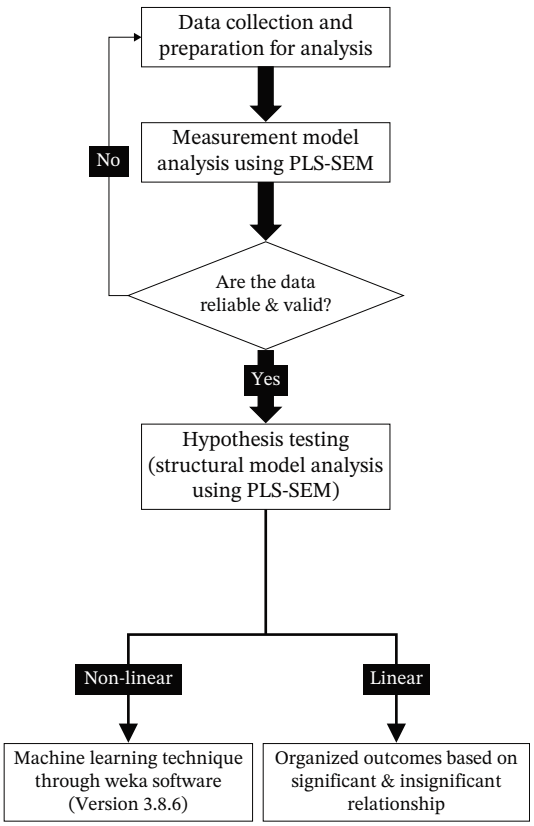


FIGURE 2 | Flow of research.

2.4 | Measures

All the measuring constructs were adapted from prior literature. In this study, the exogenous variables were divided into firm (ISP and MSP) and user factors (PSs and BSs). A four-item scale of ISP and an item scale of MSP were adapted from Hwang et al. [31]. A three-item scale of PS was adapted from Alqahtani [39]. Similarly, a three-item scale of BS was adapted from Alqahtani [39]. A five-item scale of CA was adapted from Hwang et al. [31]. Likewise, a six-item scale of CC was adapted from Hwang et al. [31]. Finally, a four-item scale of EPB was adapted from Yao et al. [52]. A seven-point Likert scale was used to measure the constructs. Furthermore, the latent variable scores of all constructs were used for ML analysis. This allowed the ML analysis to perform at validated construct level rather than at the raw-item levels.

3 | Analysis and Results

3.1 | Descriptive Analysis

Before beginning data analysis, multivariate assumptions were checked to confirm the dataset's quality. According to Hair et al. [50], multivariate approaches demand that the dataset meet a number of statistical assumptions, including outlier detection, multicollinearity, and normality. To detect multivariate outliers, Mahalanobis D2 was used with a cut-off value greater than 4 [50]. For multicollinearity, a thorough

hbet, 2026, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/hbe2/2009721 by Rao Faizan Ali - University Of Texas Md Anderson Cancer Center , Wiley Online Library on [25/09/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

TABLE 2 | Descriptive analysis.

Variables	Mean	Standard Deviation	Skewness	Kurtosis
ISP	4.066	1.920	−0.050	−1.310
MSP	3.975	1.904	0.002	−1.281
PS	4.652	1.811	−0.439	−0.909
BS	4.629	1.828	−0.277	−1.068
CA	4.167	2.006	−0.133	−1.332
CC	4.134	1.913	−0.023	−1.305
EPB	4.104	1.800	−0.078	−1.041

collinearity analysis was performed as recommended by Hair et al. [53], and the findings revealed that all constructs had values less than 5. Normality was determined by skewness and kurtosis, with all values falling within the ±2 threshold limit [54] as shown in Table 2.

Furthermore, common method bias (CMB), which can influence research findings in behavioral sciences, was discussed. Following Podsakoff et al. [55], a Harman single-factor test was conducted. The test found that the highest variation explained by a single component was roughly 37%, which is significantly lower than the 50% threshold, showing that CMB is not an issue in this study.

3.2 | Structural Equation Modeling

Hair et al. [56] suggested the use of SmartPLS to implement the PLS-SEM approach. PLS-SEM gives consistent and thorough explanations for actual phenomena, and it outperforms regression analysis [50]. PLS-SEM analysis comprises measurement and structural models, which are explained in detail below.

3.2.1 | Measurement Model

The measurement model summarizes the findings regarding construct reliability and validity. The next sections provide extensive detail about both convergent and discriminant validity. In addition, information on factor loadings and variance inflation factors (VIF) is provided.

3.3 | Reliability and Validity

Table 3 indicates the results of the reliability and convergent validation analysis of various study variables and their corresponding items. Two reliability indicators were used: Cronbach's α and composite reliability (CR). Hair et al. [53] recommend an acceptable threshold value of CR and Cronbach's α of ≥0.70 for appropriate results. However, a CR value of 0.60–0.70 is regarded as adequate [56].

In the PLS-SEM literature, the major measures of convergent validity are average variance extracted (AVE) and item loading [56]. Hair et al. [53] suggest an excellent item loading threshold of ≥0.708. However, if the item loading is between 0.4 and 0.7, the construct can still be kept provided the AVE is ≥0.5 [56]. The AVE threshold value is >0.5. According to the results shown in Table 3, all constructs and their accompanying items enacted the minimum threshold requirements.

3.4 | Discriminant Validity

Prior research has identified cross-loading, Fornell–Larcker, and the heterotrait–monotrait ratio of correlation (HTMT) as the most commonly used approaches for measuring discriminant validity. However, Henseler et al. [57] contend that cross-loading and Fornell–Larcker may not be the most effective methods for determining discriminant validity in PLS-SEM. As a result, the HTMT criterion was chosen as the preferred strategy in the current investigation. According to Hair et al. [50], HTMT levels should be less than 0.90. As shown in Table 4, the discriminant validity results for each variable show that all HTMT values fall effectively below the 0.90 criterion.

3.5 | Structural Model

3.5.1 | Hypotheses Analysis

To determine the statistical significance between study variables ($p < 0.05$), the path estimation method used the bootstrapping technique with 5000 resampling at one-tailed. Table 5 presents the hypothesis analysis.

Table 5 shows the association between exogenous variables (ISP, MSP, PS, and BS) CA, and CC. The results indicated that ISP has a positive and significant relationship with CA (Hypothesis 1a: $\beta = 0.247$, $t-\text{value} = 3.330$, $p = 0.001$) but an insignificant relationship with CC (Hypothesis 1b: $\beta = 0.045$, $t-\text{value} = 0.694$, $p = 0.488$). Thus, Hypothesis 1a was accepted, and Hypothesis 1b was rejected. Surprisingly, the analysis indicated that MSP has an insignificant relationship with CA (Hypothesis 2a: $\beta = 0.004$, $t-\text{value} = 0.071$, $p = 0.943$) but a significant association with CC (Hypothesis 2b: $\beta = 0.235$, $t-\text{value} = 3.303$, $p = 0.001$). Therefore, Hypothesis 2a was rejected, and Hypothesis 2b was accepted. Moreover, the analysis demonstrated that PS had an insignificant relationship with CA (Hypothesis 3a: $\beta = 0.112$,

hbet, 2026, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/hbe2/2009721 by Rao Faizan Ali - University Of Texas Md Anderson Cancer Center , Wiley Online Library on [25/09/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

TABLE 3 | Reliability and validity.

Variables	Items	Loading	VIF	Cronbach's alpha	CA	AVE
Information security policy	ISP1	0.885	2.713	0.903	0.932	0.775
	ISP2	0.880	2.485			
	ISP3	0.883	2.670			
	ISP4	0.873	2.679			
Management security practices	MSP1	0.901	2.130	0.859	0.913	0.778
	MSP2	0.885	2.332			
	MSP3	0.861	2.075			
Password security	PS1	0.832	1.551	0.750	0.857	0.666
	PS2	0.826	1.506			
	PS3	0.790	1.455			
Brower security	BS1	0.806	1.349	0.744	0.853	0.660
	BS2	0.813	1.599			
	BS3	0.818	1.598			
Cybersecurity awareness	CA1	0.855	2.563	0.917	0.937	0.750
	CA2	0.859	2.603			
	CA3	0.867	2.634			
	CA4	0.883	2.918			
	CA5	0.865	2.613			
Cybersecurity compliance	CC1	0.852	2.599	0.927	0.943	0.732
	CC2	0.848	2.637			
	CC3	0.852	2.716			
	CC4	0.872	2.863			
	CC5	0.855	2.742			
	CC6	0.854	2.579			
Employee proactive behavior	EPB1	0.797	1.688	0.797	0.868	0.623
	EPB2	0.830	1.839			
	EPB3	0.835	1.755			
	EPB4	0.687	1.336			

$t-$value = 1.261, $p = 0.207$) but a significant relationship with CC (Hypothesis 3b: $\beta = 0.248$, $t-$value = 2.724, $p = 0.006$). Thus, Hypothesis 3a was rejected, and Hypothesis 3b was accepted. On the other hand, BS has a significant relationship with CA (Hypothesis 4a: $\beta = 0352$, $t-$value = 3.680, $p = 0.001$) and CC (Hypothesis 4b: $\beta = 0.235$, $t-$value = 2.311, $p = 0.021$). Therefore, Hypothesis 4a and Hypothesis 4b were supported and accepted. Unexpectedly, the relationship between CA and CC was insignificant (Hypothesis 5: $\beta = 0.046$, $t-$value = 0.702, $p = 0.483$). Therefore, Hypothesis 5 was rejected. Furthermore, the association between CA and EPB was positive and significant (Hypothesis 6: $\beta = 0.259$, $t-$value = 3.254, $p = 0.001$).

hbet, 2026, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/hbe2/2009721 by Rao Faizan Ali - University Of Texas Md Anderson Cancer Center , Wiley Online Library on [25/09/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

TABLE 4 | Discriminant validity (HTMT).

Variables	ISP	MSP	PS	BS	CA	CC	EPB
ISP	**0.880**						
MSP	0.450	**0.882**					
PS	0.486	0.469	**0.816**				
BS	0.565	0.527	0.153	**0.812**			
CA	0.501	0.335	0.600	0.677	**0.866**		
CC	0.399	0.511	0.675	0.686	0.426	**0.856**	
EPB	0.620	0.530	0.444	0.471	0.399	0.364	**0.789**

Note: Values in diagonal are the square root of AVE.

TABLE 5 | Hypothesis analysis.

Hypothesis	*β*-value	*t*-statistics	CI (2.50%-97.50%)	*p* value	Decision
Hypothesis 1a: ISP➔CA	0.247	3.330	(0.102–0.391)	0.001	Accepted
Hypothesis 1b: ISP➔CC	0.045	0.694	(−0.081 to 0.171)	0.488	Rejected
Hypothesis 2a: MSP➔CA	0.004	0.071	(−0.117 to 0.129)	0.943	Rejected
Hypothesis 2b: MSP➔CC	0.235	3.303	(0.098–0.378)	0.001	Accepted
Hypothesis 3a: PS➔CA	0.122	1.261	(−0.067 to 0.314)	0.207	Rejected
Hypothesis 3b: PS➔CC	0.248	2.724	(0.072–0.431)	0.006	Accepted
Hypothesis 4a: BS➔CA	0.352	3.680	(0.158–0.533)	0.001	Accepted
Hypothesis 4b: BS➔CC	0.235	2.311	(0.038–0.428)	0.021	Accepted
Hypothesis 5: CA➔CC	0.046	0.702	(−0.074 to 0.182)	0.483	Rejected
Hypothesis 6: CA➔EPB	0.259	3.254	(0.093–0.409)	0.001	Accepted
Hypothesis 7: CC➔EPB	0.217	2.730	(0.052–0.364)	0.006	Accepted

Thus, Hypothesis 6 was accepted. Finally, the relationship between CC and EPB was positive and significant (Hypothesis 7: $\beta = 0.217$, $t - \text{value} = 2.73$, $p = 0.006$). Thus, Hypothesis 7 was accepted. Moreover, Figure 3 demonstrates the structural model.

3.6 | Predictive Analysis Using ML Algorithms

After the PLS-SEM analysis, ML algorithms were applied to assess the predictive capability of the proposed cybersecurity framework. The ML analysis was conducted using WEKA Version 3.8.6. Before performing the classification analysis, the validated latent variable scores were exported from SmartPLS and prepared for WEKA. EPB was specified as the target/class variable, whereas the remaining constructs were treated as predictor attributes. Specifically, two predictive models were tested. First, CA and CC were used to classify EPB. Second, firm-level technical factors and user-level social factors were used to classify EPB. Since the purpose of the ML analysis was classification, EPB was transformed into nominal classes before importing the data into WEKA. Following prior hybrid SEM–ML procedures, the target construct was categorized into low, medium, and high levels using the mean ± SD criterion, whereas the predictor attributes were retained as numeric latent variable scores. This classification procedure enabled the study to examine whether the validated STS-based constructs could accurately classify different levels of EPB.

A 10-fold cross-validation procedure was used to evaluate model stability and reduce the risk of overfitting [58]. In this procedure, the dataset was divided into 10 approximately equal subsets. In each round, nine subsets were used to train the model, whereas the remaining subset was used for testing. The process was repeated 10 times until each subset had been used once as the testing set. The final predictive performance was obtained by averaging the results across the 10 folds. This procedure is widely used in WEKA-based classification studies because it provides a more reliable estimate of model performance, particularly when the sample size is moderate [51, 58, 59].

Several classifiers were applied, including BayesNet, Logistic, AdaBoostM1, OneR, LWL, and J48 [51]. These classifiers represent different learning approaches, including probabilistic learning, linear classification, ensemble learning, rule-based learning, locally weighted learning, and decision tree classification. The classifiers were evaluated using correctly classified instances, true positive rate, false positive rate, precision, recall, and F-measure [59]. Correctly classified instances indicate

hbet, 2026, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/hbe2/2009721 by Rao Faizan Ali - University Of Texas Md Anderson Cancer Center , Wiley Online Library on [25/09/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

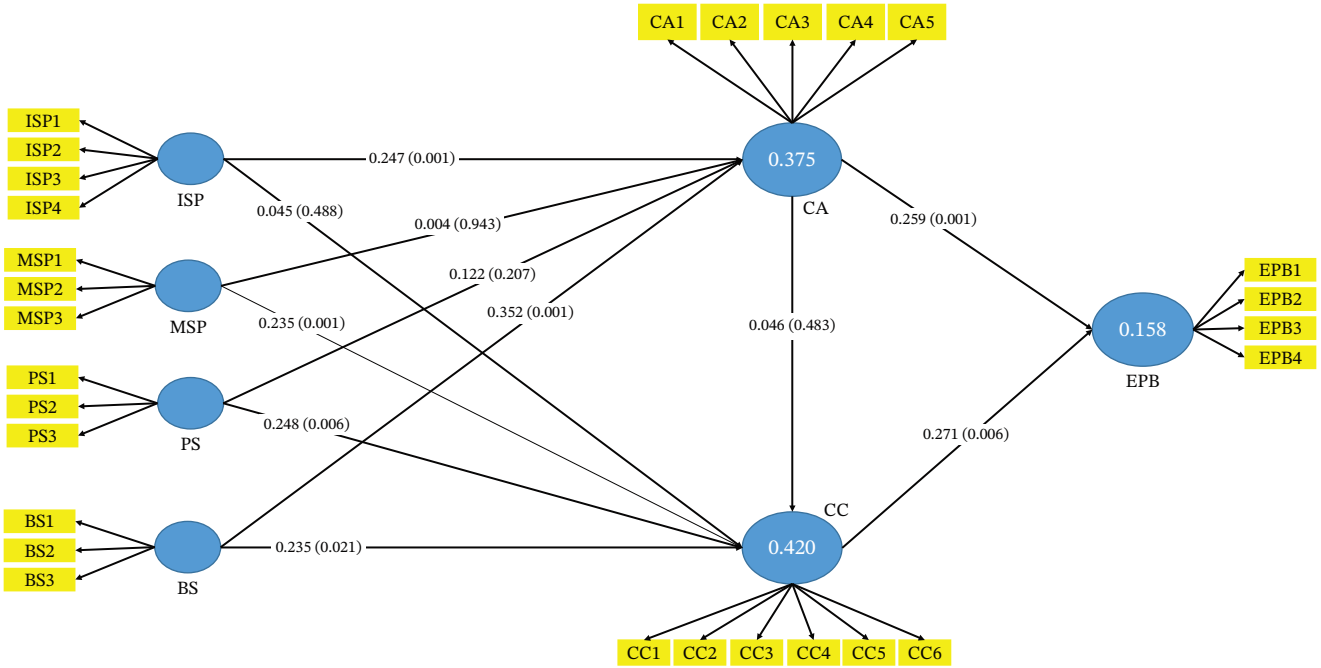


FIGURE 3 | Structural model.

TABLE 6 | Predicting EPB by CA and CC.

Classifier	CCI1 (%)	TP2 rate	FP3 rate	Precision	Recall	*F*-measure
BayesNet	77.33	0.773	0.453	0.771	0.711	0.624
Logistic	78.92	0.789	0.513	0.780	0.783	0.756
LWL	75.85	0.758	0.559	0.753	0.757	0.711
AdaBoostM1	79.06	0.790	0.637	0.791	0.699	0.801
OneR	77.52	0.775	0.613	0.770	0.735	0.633
J48	80.13	0.801	0.668	0.800	0.797	0.81

Abbreviations: CCI, correctly classified instances; FP, false positive; LWL, locally weighted learning; TP, true positive.

overall classification accuracy, whereas precision, recall, and *F*-measure provide additional information about classification quality [58, 59]. The best performing classifier was identified based on the highest overall predictive performance across these metrics.

Table 6 presents the classification performance of CA and CC in predicting EPB. The results highlight that J48 achieved the strongest predictive performance among tested classifiers, which correctly classified instances of 80.13%, a true positive rate of 0.801, precision of 0.800, recall of 0.797 and *F*-measure of 0.81. The findings affirmed that CA and CC have meaningful predictive relevance for EPB.

Moreover, Table 7 highlights the classification performance of firm-level and user-level factors in predicting EPB. The ML outcomes highlight that J48 again performed better than the other classifiers, achieving 85.79% correctly classified instances, with a true positive rate of 0.857, precision of 0.833, recall of 0.838, and *F*-measure of 0.812. These outcomes provide predictive support for the integrated STS framework by showing that ISP, MSP, PS, and BS collectively classify EPB with relatively high accuracy.

4 | Discussion and Conclusion

4.1 | Discussion on Findings

The prime objective of this study was to examine how user-level (PS and BS) and firm-level (ISP and MSP) factors jointly impact CA, compliance, and EPB in the I5.0 context. The research framework was anchored on STS theory. The hypothesized relationships were examined through a novel PLS-SEM and ML technique.

To achieve the research objectives, seven hypotheses (Hypothesis 1–Hypothesis 7) were proposed and analyzed through the PLS-SEM approach. Concerning the role of firm factors (ISP and MSP) on cybersecurity practices (CC and CA), two hypotheses (Hypothesis 1a,b and Hypothesis 2a,b) were proposed. The outcomes indicate that ISP has a positive relationship with CA (Hypothesis 1a) and MSP positively promotes CC (Hypothesis 2b). The outcomes are supported by past studies. For instance, Hwang et al. [31] confirmed that security policies significantly and positively promote security awareness. From the STS perspective, firm cybersecurity policies represent formal structures

hbet, 2026, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/hbe2/2009721 by Rao Faizan Ali - University Of Texas Md Anderson Cancer Center , Wiley Online Library on [25/09/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

TABLE 7 | Predicting EPB by ISP, MSP, PS, and BS.

Classifier	CCI1 (%)	TP2 rate	FP3 rate	Precision	Recall	*F*-measure
BayesNet	79.51	0.795	0.563	0.793	0.617	0.732
Logistic	82.37	0.823	0.624	0.811	0.722	0.711
LWL	79.15	0.791	0.553	0.716	0.763	0.692
AdaBoostM1	80.63	0.806	0.613	0.702	0.789	0.753
OneR	81.55	0.815	0.628	0.821	0.806	0.786
J48	85.79	0.857	0.647	0.833	0.838	0.812

that define and guide employee understanding of cyber risk. Effective policies serve as a cognitive framework through which employees interpret cybersecurity requirement [22]. In this sense ISP is a technical enabler that shapes the social subsystems, reinforcing the interconnected nature of sociotechnical systems. Another explanation for this result could be that the ISP creates a structured framework that emphasizes the significance of complying with cybersecurity protocols by educating people about risks and appropriate behavior through the use of clear instructions and standards. From I5.0 context, both relationships are strengthened by human-centric orientation. In highly digitalized environment, employees need clear and adaptive security policies to understand the evolving cyber security risks. Thus, Hypothesis 1a and Hypothesis 2b were accepted. Unexpectedly, ISP and MSP have an insignificant relationship with CC (Hypothesis 1b) and CA (Hypothesis 2a). From STS perspective, these unexpected outcomes highlight a misalignment between social and technical subsystems. Specifically, ISP represent a technical systems and remain symbolic in emerging economies like Malaysia and fail to drive the actual compliance. Likewise, MSP may not promote awareness because it is a social-cognitive process and develop through learning, communication, and experience. From human-centric principle of I5.0 highlight that human are active decision-makers rather than passive recipients of policies and managerial directives. Consequently, top-down policies and actions are insufficient unless they are adaptive, engaging and aligned with employee routines and digital technologies.

Concerning the role of user factors (PS and BS) in promoting cybersecurity practices (CA and CC), two hypotheses (Hypothesis 3a,b and Hypothesis 4a,b) were formulated. Surprisingly, the outcomes indicated that PS has an insignificant impact on CA (Hypothesis 3a). One explanation for these results could be that although people are aware of the risks associated with cybersecurity, they often prioritize convenience ahead of security when setting up passwords. Even when people are aware of the risks, they may nevertheless reuse passwords or engage in other weak password behaviors as a result of this knowledge gap. Thus, Hypothesis 3a was rejected. On the other hand, the results indicated that PS has a positive relationship with CC (Hypothesis 3b), and BS has a positive relationship with CA and CC (Hypothesis 4a,b). These outcomes are supported by past studies [39]. This intriguing outcome might be explained by the fact that PS and BS are the primary entrance points for securing sensitive data, and understanding their vulnerabilities encourages users to adopt more compact security measures. Users who acknowledge the risks connected to weak passwords and insecure browsers are more likely to follow security practices, like choosing strong passwords and changing browser settings, which improves overall cybersecurity. Thus, Hypothesis 3b and Hypothesis 4a,b were accepted.

Furthermore, the study results affirmed that CA has an insignificant association with CC (Hypothesis 5). The insignificant relationship between CA and CC provides an important theoretical insight. Although CA reflects employees' knowledge of cyber risks, policies, and safe digital practices, such awareness does not automatically translate into compliant behavior. This finding indicates the presence of an awareness-action gap in cybersecurity behavior. Employees may understand cyber threats but may still fail to comply due to convenience-seeking behavior, weak enforcement, time pressure, lack of monitoring, or limited perceived consequences for noncompliance. From the STS perspective, this result suggests that the social subsystem, represented by employee cognition and awareness, must be supported by technical and organizational control mechanisms before it can produce consistent compliance. In other words, awareness alone is insufficient unless it is reinforced through clear policies, managerial follow-up, secure system design, compliance monitoring, and repeated behavioral training. In the I5.0 context, this finding is particularly relevant because human-centric digital systems require employees not only to be aware of cyber risks but also to internalize cybersecurity routines as part of daily human–machine interaction. Thus, Hypothesis 5 was rejected. Finally, the results revealed that CA and CC have a positive and significant relationship with EPB (Hypothesis 6 and Hypothesis 7). The outcomes are in line with past studies. To explain the findings that CA and CC positively enhance EPB by providing personnel with knowledge of potential risks and clear action plans, encouraging them to take the initiative in preventing threats. This combination encourages a sense of responsibility and attentiveness in employees, encouraging them to actively participate in securing their workplace beyond simply compliance. Thus, Hypothesis 6 and Hypothesis 7 were accepted.

4.2 | Research Contributions

4.2.1 | Theoretical Contributions

The outcomes of this research have both theoretical contributions and practical implications. The study findings have threefold theoretical contribution. First, the study fulfills the gap in

hbet, 2026, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/hbe2/2009721 by Rao Faizan Ali - University Of Texas Md Anderson Cancer Center , Wiley Online Library on [25/09/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

the literature on cybersecurity by incorporating STS theory into the I5.0 framework. Previous research has mostly examined the technical factors, refraining from considering the relationship between these variables and user factors. By investigating user and firm characteristics concurrently that affect CA, compliance, and proactive staff behavior, this study closes the knowledge gap. Second, by emphasizing the value of cooperatively optimizing socio-technical components in advancing cybersecurity practices, this work advances STS theory. It provides a comprehensive framework that highlights the interplay between technological and human elements, especially in the Malaysian manufacturing sector where there is a dearth of cybersecurity research. Third, this study contributes methodologically by integrating PLS-SEM and ML in cybersecurity research. Unlike past studies that rely only on SEM-based explanatory modeling, this study combines theory testing with predictive classification. PLS-SEM confirms the explanatory relationships derived from STS theory, whereas ML evaluates whether the exogenous factors can predict EPB. This dual analytical approach advances cybersecurity research by demonstrating that cybersecurity frameworks should be assessed not only through statistical significance but also through their predictive usefulness for identifying proactive employee behavior.

4.2.2 | Practical Implications

For managers, cybersecurity officers, HR departments, and legislators at Malaysian manufacturing companies, the results offer a number of useful implications. First, businesses ought not to perceive security policies as static documents given the strong association between ISP and cybersecurity knowledge. Instead, managers should use role-based cybersecurity guidelines, brief policy briefings, onboarding sessions, visual reminders, and recurring policy-refresh training to turn rules into practical awareness routines. Employees should be fully aware of the policy requirements, its significance, and how it affects their everyday interactions with digital systems, browsers, passwords, and company data. Second, the substantial impact of MSP on CC suggests that managerial participation is necessary to translate cybersecurity expectations into real behavior. Periodic cybersecurity briefings, recurring compliance audits, departmental-level cybersecurity checklists, and supervisor-led follow-up on threatening activities are all examples of management-led cybersecurity procedures that manufacturing companies should use. Third, organizations should improve employee-level digital health through targeted technological and behavioral interventions, pursuant to browser and PS. Organizations should employ multi-factor authentication, promote the use of authorized password managers, restrict sharing passwords, and, where necessary, mandate regular password changes. Fourth, the insignificant relationship between CA and CC highlights that firms should combine awareness programs with practical cybersecurity simulation training, incident-response drills, and scenario-based learning. These will help employees to identify suspicious threats, avoid unsafe browsing behavior and respond to possible cyber incidents. Lastly, organizations should foster a supportive reporting culture where employees are encouraged to report suspicious emails, system anomalies, password-related concerns, and unsafe digital practices without fear of blame, as both CA and CC greatly encourage EPB.

5 | Limitations and Future Directions

This study has various limitations that lay the foundation for future research direction. First, the study utilized a quantitative and cross-sectional survey methodology, which means it cannot completely reflect how cybersecurity knowledge, compliance, and proactive behavior vary over time. Future research may use longitudinal designs to investigate the evolution of cybersecurity behavior following training, cyber events, or technical advancements. Second, the study used self-reported data, which may have been influenced by social desirability bias because CC and proactive behavior are sensitive organizational concerns. Confidentiality was maintained, and CMB was statistically tested. Future studies may integrate survey data with objective indications like as training records, phishing simulation outcomes, compliance audits, password-update logs, incident reports, or system-generated security data. Third, convenience sampling was selected since cybersecurity-related data is sensitive and access to manufacturing staff is limited. However, this strategy may restrict representativeness and introduce selection bias since employees who were more available or willing to participate may differ from those who did not. Therefore, the findings should be generalized with caution beyond the studied Malaysian industrial personnel. To increase representativeness, future study could utilize probability sampling, stratified sampling, or multistage samples across various Malaysian regions, manufacturing subsectors, and company sizes. Fourth, the study was restricted to Malaysian manufacturing companies; cybersecurity practices may vary across country cultures, industries, and regulatory frameworks. In addition to conducting cross-national comparison studies, future study may test the concept in industries including healthcare, banking, education, logistics, construction, and public organizations.

Funding

This study was supported by the University of Kent (10.13039/501100001316).

Ethics Statement

All procedures of this study adhere to the Declaration of Helsinki and the Measures for the Ethical Review of Life Science and Medical Research Involving Human. Specifically, this study is not medical research and does not involve human experimentation as defined in the Declaration of Helsinki, and the questions in the questionnaire have no adverse effect on the mental health status of the respondents. This study uses anonymized data to conduct research, causing no harm to the human body and involving neither sensitive personal information nor commercial interests. According to the regulations of the authors' institution, ethical approval is not required for this questionnaire-based study.

Consent

Prior to the commencement of the study, informed consent was obtained from all participants, ensuring their voluntary participation and comprehension of the study's purpose, objectives, and data utilization methods. The participants were provided with detailed information regarding the nature and objectives of the study, and they voluntarily agreed to participate without any coercion or undue influence.

hbet, 2026, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/hbe2/2009721 by Rao Faizan Ali - University Of Texas Md Anderson Cancer Center , Wiley Online Library on [25/09/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

Data will be available on request from the corresponding author.

References

1. G. Czeczot, I. Rojek, D. Mikołajewski, and B. Sangho, "AI in IIoT Management of Cybersecurity for Industry 4.0 and Industry 5.0 Purposes," *Electronics* 12, no. 18 (2023): 3800, https://doi.org/10.3390/electronics12183800.

2. I. Ahmed, N. U. I. Hossain, S. A. Fazio, M. Lezzi, and M. S. Islam, "A Decision Support Model for Assessing and Prioritization of Industry 5.0 Cybersecurity challenges," *Economics* 3 (2024): 100018, https://doi.org/10.1016/j.smse.2024.100018.

3. S. Kaur, K. Ali, and K. Shirahada, "Redefining Sustainability Through Dual-Servitization and Circular Economy in Industry 5.0," *Total Quality Management & Business Excellence* 37, no. 1-2 (2026): 72–95, https://doi.org/10.1080/14783363.2025.2607455.

4. R. Kour, R. Karim, P. Dersin, and N. Venkatesh, "Cybersecurity for Industry 5.0: Trends and gaps," *Science* 6 (2024): 1434436, https://doi.org/10.3389/fcomp.2024.1434436.

5. A. Alqudhaibi, M. Albarrak, S. Jagtap, N. Williams, and K. Salonitis, "Securing Industry 4.0: Assessing Cybersecurity Challenges and Proposing Strategies for Manufacturing Management," *Cyber Security and Applications* 3 (2024): 100067, https://doi.org/10.1016/j.csa.2024.100067.

6. Statista, *Global Companies Financial Loss to Cyberattacks 2024* (Statista, 2024), https://www.statista.com/statistics/1475047/companies-worldwide-financial-loss-to-cyberattacks/#:%7E:text=As%2520of%2520February%25202024%252C%2520over,least%2520one%2520million%2520U.S.%2520dollars.

7. IBM, *Cost of a Data Breach 2024* (2024): IBM, https://www.ibm.com/reports/data-breach.

8. SAS, *SAS Cyber Attack – Update* (SAS, 2023), https://www.sasgroup.net/newsroom/press-releases/2023/sas-cyber-attack--update/.

9. D. J. Thapa, "Cyber Attacks in Saudi Arabia: Major Concern for Middle-East," (Threatcop, 2024), https://threatcop.com/blog/cyber-attacks-in-saudi-arabia/.

10. M. Kokila, and S. Reddy, "Authentication, Access Control and Scalability Models in Internet of Things Security - a Review," *Cyber Security and Applications* 3 (2024): 100057, https://doi.org/10.1016/j.csa.2024.100057.

11. Manpower, "The IT World of Work: Insights and Outlook for 2025," in *Manpower Group* (2025), https://www.manpowergroup.com/en/insights/blogs/the-it-world-of-work-insights-and-outlook-for-2025.

12. "Malaysia's Digital Growth and Geopolitics Widen Cyber Attack Surface, Raising Critical Infrastructure Risks," *Industrial Cyber* (2026), https://industrialcyber.co/reports/malaysias-digital-growth-and-geo-politics-widen-cyber-attack-surface-raising-critical-infrastructure-risks.

13. S. Badi, and M. Nasaj, "Cybersecurity Effectiveness in UK Construction Firms: An Extended McKinsey 7S Model Approach," *Engineering, Construction and Architectural Management* 31, no. 11 (2024): 4482–4515, https://doi.org/10.1108/ECAM-12-2022-1131.

14. N. O. Qatanani, M. Alghababsheh, A. Aburayya, and M. Nasaj, "Factors Influencing m-Government Adoption in the Developing World: A UTAUT-Based Model Integrating Trust, Risk and Trendiness," *VINE Journal of Information and Knowledge Management Systems* 56, no. 3 (2026): 797–828, https://doi.org/10.1108/VJIKMS-10-2023-0255.

15. M. Al-Emran, M. A. Al-Sharafi, B. Foroughi, et al., "Evaluating the Barriers Affecting Cybersecurity Behavior in the Metaverse Using PLS-SEM and Fuzzy Sets (fs QCA)," *Computers in Human Behavior* 159 (2024): 108315, https://doi.org/10.1016/j.chb.2024.108315.

16. F. Fatima, J. C. Hyatt, S. U. Rehman, E. De La Cruz, G. S. Nadella, and K. Meduri, "Resilience and Risk Management in Cybersecurity: A Grounded Theory Study of Emotional, Psychological, and Organizational Dynamics," *Journal of Economy and Technology* 2 (2024): 247–257, https://doi.org/10.1016/j.ject.2024.08.004.

17. B. Kim, and M. 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," *Technology in Society* 77 (2024): 102543, https://doi.org/10.1016/j.techsoc.2024.102543.

18. Y. Hoong, D. Rezania, and R. Baker, "When Traditional SME Managers Encounter Cybersecurity: Discourse Analysis of Opportunities and Dilemmas in Meeting the Demands," *Technology in Society* 78 (2024): 102650, https://doi.org/10.1016/j.techsoc.2024.102650.

19. K. Ali, and S. K. Johl, "Driving Sustainability in Industry 5.0 Through Sociotechnical Approach of Quality Management," *Total Quality Management & Business Excellence* 35, no. 13-14 (2024): 1567–1592, https://doi.org/10.1080/14783363.2024.2375303.

20. B. Valkenburg, and I. Bongiovanni, "Unravelling the Three Lines Model in Cybersecurity: A Systematic Literature Review," *Computers & Security* 139 (2024): 103708, https://doi.org/10.1016/j.cose.2024.103708.

21. E. H. Kessler, *Encyclopedia of Management Theory*, 1st ed. (Sage Ltd, 2013).

22. M. Malatji, A. Marnewick, and S. Von Solms, "Validation of a Socio-Technical Management Process for Optimising Cybersecurity Practices," *Computers & Security* 95 (2020): 101846, https://doi.org/10.1016/j.cose.2020.101846.

23. V. Zimmermann, and K. Renaud, "Moving From a "Human-as-Problem" to a "Human-as-Solution" Cybersecurity Mindset," *International Journal of Human-Computer Studies* 131 (2019): 169–187, https://doi.org/10.1016/j.ijhcs.2019.05.005.

24. M. Sadok, C. Welch, and P. Bednar, "A Socio-Technical Perspective to Counter Cyber-Enabled Industrial Espionage," *Security Journal* 33, no. 1 (2019): 27–42, https://doi.org/10.1057/s41284-019-00198-2.

25. H. Zhang, Z. Tang, and K. Jayakar, "A Socio-Technical Analysis of China's Cybersecurity Policy: Towards Delivering Trusted e-Government Services," *Telecommunications Policy* 42, no. 5 (2018): 409–420, https://doi.org/10.1016/j.telpol.2018.02.004.

26. H. Kim, D. Shin, and D. Lee, "A Socio-Technical Analysis of Software Policy in Korea: Towards a Central Role for Building ICT Ecosystems," *Telecommunications Policy* 39, no. 11 (2015): 944–956, https://doi.org/10.1016/j.telpol.2015.09.001.

27. L. M. Bishop, P. M. Asquith, and P. L. Morgan, "The Employee Cybersecurity Awareness Framework," *Human Behavior and Emerging Technologies* 2025, no. 1 (2025): 1025045, https://doi.org/10.1155/hbe2/1025045.

28. K. Ali, "Total Quality Management in Manufacturing Firms: Current and Future Trends," *Foresight* 26, no. 3 (2024): 505–530, https://doi.org/10.1108/fs-09-2023-0180.

29. D. Javaheri, M. Fahmideh, H. Chizari, P. Lalbakhsh, and J. Hur, "Cybersecurity Threats in Fin Tech: A Systematic Review," *Expert Systems With Applications* 241 (2023): 122697, https://doi.org/10.1016/j.eswa.2023.122697.

hbet, 2026, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/hbe2/2009721 by Rao Faizan Ali - University Of Texas Md Anderson Cancer Center , Wiley Online Library on [25/09/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

30. V. Schlatt, T. Guggenberger, J. Schmid, and N. Urbach, "Attacking the Trust Machine: Developing an Information Systems Research Agenda for Blockchain Cybersecurity," *International Journal of Information Management* 68 (2022): 102470, https://doi.org/10.1016/j.ijinfomgt.2022.102470.

31. I. Hwang, R. Wakefield, S. Kim, and T. Kim, "Security Awareness: The First Step in Information Security Compliance Behavior," *Journal of Computer Information Systems* 61, no. 4 (2019): 345–356, https://doi.org/10.1080/08874417.2019.1650676.

32. A. Chaudhuri, R. K. Behera, and P. K. Bala, "Factors Impacting Cybersecurity Transformation: An Industry 5.0 Perspective," *Computers & Security* 150 (2025): 104267, https://doi.org/10.1016/j.cose.2024.104267.

33. R. F. Ali, P. Dominic, and K. Ali, "Organizational Governance, Social Bonds and Information Security Policy Compliance: A Perspective Towards Oil and Gas Employees," *Sustainability* 12, no. 20 (2020): 8576, https://doi.org/10.3390/su12208576.

34. I. Hwang, and D. Kim, "The Effect of Organizational Information Security Environment on the Compliance Intention of Employee," *Journal of Information Systems* 25, no. 2 (2016): 51–77, https://doi.org/10.5859/kais.2016.25.2.51.

35. A. M. Asfahani, "Behind the Digital Veil: Decoding the Influence of HR Training on Information Security Awareness in Saudi Arabia," *Cogent Business & Management* 11, no. 1 (2024): , https://doi.org/10.1080/23311975.2024.2395430.

36. S. Chaudhary, "Driving Behaviour Change With Cybersecurity Awareness," *Computers & Security* 142 (2024): 103858, https://doi.org/10.1016/j.cose.2024.103858.

37. L. Wong, V. Lee, G. W. Tan, K. Ooi, and A. Sohal, "The Role of Cybersecurity and Policy Awareness in Shifting Employee Compliance Attitudes: Building Supply Chain Capabilities," *International Journal of Information Management* 66 (2022): 102520, https://doi.org/10.1016/j.ijinfomgt.2022.102520.

38. Y. Bang, D. Lee, Y. Bae, and J. Ahn, "Improving Information Security Management: An Analysis of ID–Password Usage and a New Login Vulnerability Measure," *International Journal of Information Management* 32, no. 5 (2012): 409–418, https://doi.org/10.1016/j.ijinfomgt.2012.01.001.

39. M. A. Alqahtani, "Factors Affecting Cybersecurity Awareness among University Students," *Applied Sciences* 12, no. 5 (2022): 2589, https://doi.org/10.3390/app12052589.

40. M. Nasaj, "Corporate Digital Responsibility and Green Innovation: A Strategic Model for Sustainable Competitive Advantage," in *Management Decision* (Emerald Publishing, 2026), 1–31, https://doi.org/10.1108/md-06-2025-1670.

41. I. Alhadidi, A. Nweiran, and G. Hilal, "The Influence of Cybercrime and Legal Awareness on the Behavior of University of Jordan Students," *Heliyon* 10, no. 12 (2024): e32371, https://doi.org/10.1016/j.heliyon.2024.e32371.

42. H. Taherdoost, "A Critical Review on Cybersecurity Awareness Frameworks and Training Models," *Procedia Computer Science* 235 (2024): 1649–1663, https://doi.org/10.1016/j.procs.2024.04.156.

43. M. A. Rizal, and B. Setiawan, "Information Security Awareness Literature Review: Focus Area for Measurement Instruments," *Procedia Computer Science* 234 (2024): 1420–1427, https://doi.org/10.1016/j.procs.2024.03.141.

44. N. H. A. Rahim, S. Hamid, L. M. Kiah, S. Shamshirband, and S. Furnell, "A Systematic Review of Approaches to Assessing Cybersecurity Awareness," *Kybernetes* 44, no. 4 (2015): 606–622, https://doi.org/10.1108/k-12-2014-0283.

45. M. N. K. Saunders, A. Thornhill, and P. Lewis, *Research Methods for Business Students*, 8th ed. (Pearson, 2019).

46. I. I. Etikan, S. A. Musa, and R. S. Alkassim, "Comparison of Convenience Sampling and Purposive Sampling," *American Journal of Theoretical and Applied Statistics* 5, no. 1 (2016): 1, https://doi.org/10.11648/j.ajtas.20160501.11.

47. M. Alshurideh, B. A. Kurdi, S. A. Salloum, I. Arpaci, and M. Al-Emran, "Predicting the Actual Use of m-Learning Systems: A Comparative Approach Using PLS-SEM and Machine Learning Algorithms," *Interactive Learning Environments* 31, no. 3 (2020): 1214–1228, https://doi.org/10.1080/10494820.2020.1826982.

48. M. A. Memon, H. Ting, J. Cheah, R. Thurasamy, F. Chuah, and T. H. Cham, "Sample Size for Survey Research: Review and Recommendations," *Journal of Applied Structural Equation Modeling* 4, no. 2 (2020): 1–20, https://doi.org/10.47263/JASEM.4(2)01.

49. K. Ali, S. K. Johl, A. Muneer, A. Alwadain, and R. F. Ali, "Soft and Hard Total Quality Management Practices Promote Industry 4.0 Readiness: A SEM-Neural Network Approach," *Sustainability* 14, no. 19 (2022): 11917, https://doi.org/10.3390/su141911917.

50. J. F. Hair, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 3rd ed. (Sage Ltd, 2021).

51. I. Arpaci, "A Hybrid Modeling Approach for Predicting the Educational Use of Mobile Cloud Computing Services in Higher Education," *Computers in Human Behavior* 90 (2018): 181–187, https://doi.org/10.1016/j.chb.2018.09.005.

52. X. Yao, M. Li, and H. Zhang, "Suffering Job Insecurity: Will the Employees Take the Proactive Behavior or Not?," *Frontiers in Psychology* 12 (2021): 731162, https://doi.org/10.3389/fpsyg.2021.731162.

53. J. F. Hair, P. N. Sharma, M. Sarstedt, C. M. Ringle, and B. D. Liengaard, "The Shortcomings of Equal Weights Estimation and the Composite Equivalence Index in PLS-SEM," *European Journal of Marketing* 58, no. 13 (2024): 30–55, https://doi.org/10.1108/ejm-04-2023-0307.

54. D. George, and P. Mallery, "IBM SPSS Statistics 26 Step by Step," *Routledge eBooks* 10 (2019): 9780429056765, https://doi.org/10.4324/9780429056765.

55. P. M. Podsakoff, S. B. MacKenzie, J. Lee, and N. P. Podsakoff, "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* 88, no. 5 (2003): 879–903, https://doi.org/10.1037/0021-9010.88.5.879.

56. J. F. Hair, J. J. Risher, M. Sarstedt, and C. M. Ringle, "When to Use and How to Report the Results of PLS-SEM," *European Business Review* 31, no. 1 (2018): 2–24, https://doi.org/10.1108/ebr-11-2018-0203.

57. J. Henseler, C. M. Ringle, and M. Sarstedt, "A New Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modeling," *Journal of the Academy of Marketing Science* 43, no. 1 (2014): 115–135, https://doi.org/10.1007/s11747-014-0403-8.

58. M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten, "The WEKA Data Mining Software," *ACM SIGKDD Explorations Newsletter* 11, no. 1 (2009): 10–18, https://doi.org/10.1145/1656274.1656278.

59. B. A. Kurdi, M. Alshurideh, M. Nuseir, A. Aburayya, and S. A. Salloum, "The Effects of Subjective Norm on the Intention to Use Social Media Networks: An Exploratory Study Using PLS-SEM and Machine Learning Approach," in *Advances In Intelligent Systems And Computing* (Springer International Publishing, 2021), 581–592, https://doi.org/10.1007/978-3-030-69717-4_55.

hhet, 2026, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/hbet/2209721 by Rao Faizan Ali - University Of Texas Md Anderson Cancer Center , Wiley Online Library on [25/09/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License