INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

Cybersecurity Behavior in the West Sumatra Universities

Gushelmi [a,b], Rodziah Latih [b,*], Abdullah Mohd. Zin [c]

[a] Faculty of Computer Science, Universitas Putra Indonesia YPTK, Padang, West Sumatra, Indonesia
[b] Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia
[c] Faculty of Computing and Multimedia, Universiti Poly-Tech Malaysia, Kuala Lumpur, Malaysia
Corresponding author: *rodziah.latih@ukm.edu.my

***Abstract*— User cybersecurity behavior refers to the actions, habits, and decisions made by individuals when using technology and information that affect the level of security of the data and systems they access. Previous research has shown that user cybersecurity behavior is one of the leading causes of computer and information security issues in many organizations, particularly education. To address this issue, researchers must find solutions to improve user cybersecurity behavior within an organization. Therefore, this study aims to find the factors influencing user cybersecurity behavior in higher education institutions in West Sumatra in 2020. This study was conducted using a survey research method. A questionnaire was distributed to 155 respondents. The questionnaire consisted of 28 questions covering seven factors influencing user cybersecurity behavior. The survey data will be analyzed using the Structural Equation Model based on Partial Least Square. The research findings indicate that all variables, such as Misuse Prevention and Compliance, Body of Knowledge, Skill, Behavioral Intervention, Attitude, Security Compliance Behavior, and Technology, have significant relationships. The relationships between these factors will be shown in the framework to be developed. This indicates that the education sector in Indonesia is aware of cyber threats and the importance of security procedures in the workplace. For further research, a deeper exploration of specific security issues is needed to propose potential solutions or actions that can be implemented to improve user cybersecurity behavior in the education sector, particularly in Indonesia.**

***Keywords*— User cybersecurity; behavior; universities.**

Manuscript received 12 Apr. 2024; revised 9 Aug. 2024; accepted 25 Oct. 2024. Date of publication 30 Nov. 2024.

I. INTRODUCTION

Numerous facets of human existence have changed due to ICT and communication technology. It has simplified corporate procedures and has been implemented in numerous sectors. Cybercrime is one of the unforeseen effects of ICT, though. Cyberbullying, cyber fraud, spam, ransomware, trolling, phishing, identity theft, and denial of service are examples of cybercrime [1], [2].

One of the most prevalent categories of cybercrime is thought to be cyberbullying. It encompasses all types of online harassment, such as doxing, posting someone else's private information online, home address stalking, sexual harassment, framing, breaking into someone else's social media accounts, and posting on their behalf [3].

Identity theft is the second most prevalent kind of cybercrime, in which someone obtains our personal information and uses it without our permission to take money, open credit accounts, file claims for health insurance, and other purposes [4]. Ransomware is the third most prevalent category of cybercrime. This particular type of malware is designed to block access to a system or data until the attacker receives the demanded payment [5]. It is directed at businesses, governments, and consumers. WannaCry is one instance of ransomware that impacted several systems globally in 2017 [6]. Until the victim pays the ransom to obtain the decryption key, users are unable to access files or systems [7].

Information security and computer issues in businesses are influenced by a variety of factors [8]. User cybersecurity behavior is the primary contributor, accounting for around 95% of the issues [9]. All user behavior about computer system security is called user cybersecurity behavior. Encryption, smart cards, firewalls, and biometric technology [10]. are insufficient to provide sufficient information security if the organization's user cybersecurity behavior is still low [11]. But most firms aren't paying much attention to user cybersecurity behavior [11].

Examples of poor user cybersecurity practices that might leave a company vulnerable to cybercrimes include

cyberloafing, exchanging passwords with other parties, and neglecting to update antivirus software. Cyberloafing uses company computers and the Internet for private purposes [12], [13]. Researchers must first ascertain the organization's level of user security behavior to take steps to mitigate this issue. It is possible to enhance user security behavior and guarantee the computer and information security of the organization by determining the level of such behavior. This paper is organized as follows: Section 2 explains the background of the study and the methods used in making this study. Section 3 discusses the results and findings of the study. Finally, section 4 concludes the study and discusses its implications.

II. Materials and Method

A. Factors Influence User Security Behavior

Based on the considerations and the quantitative aspects of this research and its focus, non-probability sampling is considered more appropriate for selecting a sample from the population. This is because this research only conducts a case study at universities in West Sumatra, Indonesia.

The population of this study consists of all users of the university's cybersecurity system. The simple random sampling method [14] was used. The sample was randomly selected, comprising ten percent of the total population. This study determined the total population of respondents to be 1,550 people. A sample of ten percent was randomly selected, resulting in 155 respondents.

The questionnaire comprises two sections: (A) Respondent demographics and (B) Factors influencing user behavior. In section B, respondents will provide their views on the given statements by marking their answers using a 4-point Likert scale. From the hypothesized theoretical framework, there are seven factors/constructs, namely misuse prevention and compliance [15], body of knowledge [16],[17],[18], skill [19],[20], behavioral intervention [21], attitude [15],[22], compliance behavior [23],[24], and technological support [25].

This study's hypothesis is based on a literature review that addresses the relationship between the examined variables. Several hypotheses of this study are as follows:

$H1_1$: There is a significant relationship between Knowledge Base and Attitude.
$H1_0$: There is no significant relationship between knowledge base and Attitude.
$H2_1$: There is a significant relationship between Knowledge Base and Skills.
$H2_0$: There is no significant relationship between knowledge base and Skills.
$H3_1$: There is a significant relationship between Body of Knowledge and Misuse Prevention & Compliance.
$H3_0$: There is no significant relationship between Body of Knowledge and Misuse Prevention & Compliance.
$H4_1$: There is a significant relationship between Skill and Attitude.
$H4_0$: There is no significant relationship between Skill and Attitude.
$H5_1$: There is a significant relationship between Misuse Prevention & Compliance and Attitude.
$H5_0$: There is no significant relationship between Misuse Prevention & Compliance and Attitude.
$H6_1$: There is a significant relationship between Body of Knowledge and Compliance Behavior.
$H6_0$: There is no significant relationship between Body of Knowledge and Compliance Behavior.
$H7_1$: There is a significant relationship between Attitude and Compliance Behavior.
$H7_0$: There is no significant relationship between Attitude and Compliance Behavior.
$H8_1$: There is a significant relationship between Attitude and Behavioral Intervention
$H8_0$: There is no significant relationship between Attitude and Behavioral Intervention.
$H9_1$: There is a significant relationship between Behavioral Intervention and Compliance Behavior.
$H9_0$: There is no significant relationship between Behavioral Intervention and Compliance Behavior.
$H10_1$: There is a significant relationship between Technology and Misuse Prevention & Compliance.
$H10_0$: There is no significant relationship between Technology and Misuse Prevention & Compliance.
$H11_1$: Skills serve as an intermediary between Knowledge and attitudes.
$H11_0$: Skills do not serve as an intermediary between Knowledge and attitudes.
$H12_1$: Prevention of Abuse & Compliance is an intermediary between Knowledge and attitudes.
$H12_0$: Prevention of Abuse & Compliance is not an intermediary between Knowledge and attitudes.
$H13_1$: Knowledge serves as an intermediary between Attitudes and Safety Compliance Behavior.
$H13_0$: Knowledge does not serve as an intermediary between Attitudes and Safety Compliance Behavior.
$H14_1$: Attitudes are an intermediary between Behavioral Interventions and Safety Compliance Behavior.
$H14_0$: Attitudes do not serve as an intermediary between Behavioral Interventions and Safety Compliance Behavior.

To obtain the results, it will be analyzed by using the Smart SEM-PLS application version 4.0. SEM-PLS analysis is a multivariate statistical method that can be studied in making data collection-free assumptions [26], [27]. SEM (Structural Equation Model base) explores the relationship between variables and validates or rejects hypotheses. SEM-PLS estimates the regression between pending variables and isolates the error when measuring pending variables. The normality of the data distribution indicates the type of test that should be used in data analysis; that is why skewness and kurtosis tests are used in the first step of data analysis. The decision is between -2 and +2, which indicates a normal distribution. In the estimation done, the indicator data appears to be typically scattered.

The conceptual model can be visualized as shown in Fig. 1. below.

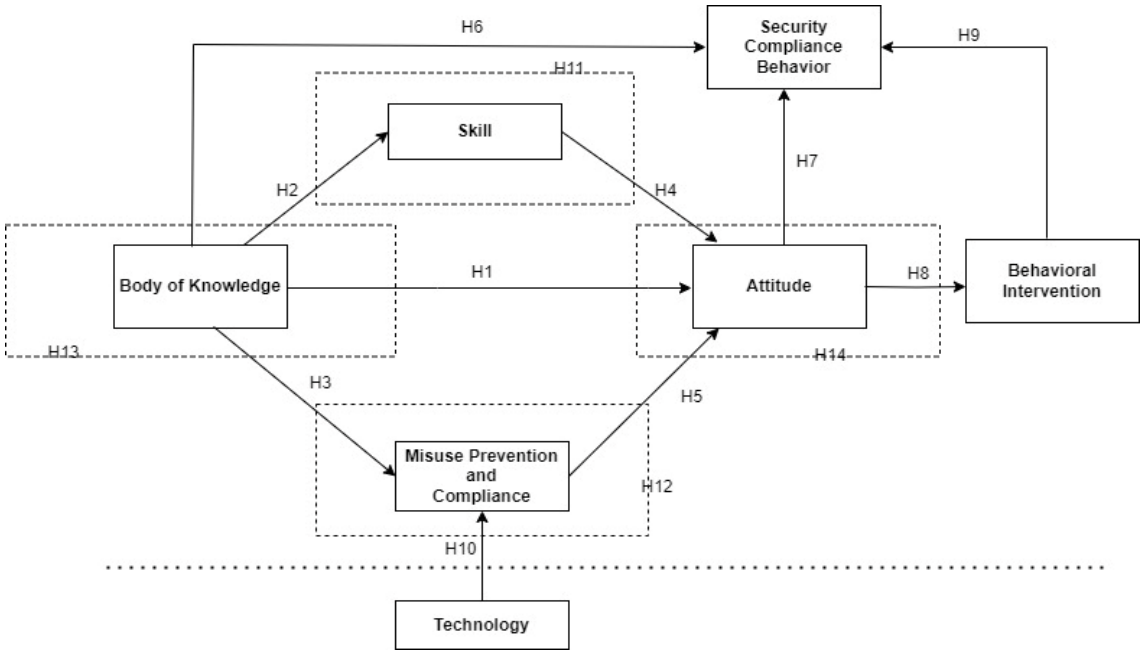

Fig. 1 Conceptual Model

The information in Table 1 shows that the skewness and kurtosis for each indicator are between -2 and +2; hence, the data distribution for each indicator is estimated to be normally distributed. Therefore, this data set can be ensured to generate valid and unbiased statistical analysis results.

TABLE I
NORMALITY ASSESSMENT

Indicators	Deviation Statistics	Kurtosis Statistics
Misuse Prevention and Compliance 1	0.494	-0.948
Misuse Prevention and Compliance 2	0.059	-0.504
Misuse Prevention and Compliance 3	0.550	-0.853
Misuse Prevention and Compliance 4	0.019	-0.595
Body of Knowledge 1	0.249	-1.963
Body of Knowledge 2	-1.041	-0.929
Body of Knowledge 3	-0.003	-0.359
Body of Knowledge 4	-0.643	-1.608
Skill 1	-0.253	-0.843
Skill 2	-0.110	-0.555
Skill 3	-0.348	-0.674
Skill 4	-0.198	-0.772
Behavior Intervention 1	-0.180	-1.371
Behavior Intervention 2	0.336	-0.867
Behavior Intervention 3	-0.390	1.005
Behavior Intervention 4	0.078	-0.929
Attitude1	0.183	0.019
Attitude 2	0.440	-1.830
Attitude 3	0.183	0.019
Attitude 4	0.412	-1.854
Compliance Behavior 1	0.205	-1.598
Compliance Behavior 2	0.525	-1.747
Compliance Behavior 3	0.015	-0.056
Compliance Behavior 4	0.179	-1.611
Technology Support1	-0.065	-0.380
Technology Support1 2	0.171	-0.476
Technology Support1 3	-0.290	-1.577
Technology Support1 4	-0.037	-0.635

III. RESULT AND DISCUSSION

A. Measurement of Relationship between Factors

1) Descriptive Statistics:

Descriptive statistics is a process used to describe the work and summarize the data concisely and clearly. The main goal is to present comprehensive information about the data's features, patterns, and relationships under observation. This is the first step in analyzing data and can provide a deep understanding of the phenomenon under study. The descriptive analysis includes minimum, maximum, standardized difference, skewness, and kurtosis statistics. Finally, descriptive analysis summarizes the main findings found in the data. It provides a better understanding of the underlying features and patterns of the phenomenon of interest.

Table 2 shows that the mean score for the factor structure for misuse prevention and compliance has a mean score of 3.12 (SD=0.48) with a skew of 0.317 and kurtosis of -0.640, Body of knowledge has a mean score of 3.51 (SD=0.36) with a skew of -0.219 and kurtosis of -0.858, Proficiency has a mean score of 3.21 (SD=0.51) with a skew of -0.105 and kurtosis of -0. 628, Behavioral interventions had a mean score range of 3.31 (SD=0.41) with a skew of 0.417 and kurtosis -0.897, Attitudes had a mean score range of 3.29 (SD=0.44) with a skew of 0.473 and kurtosis -0. 902, Security compliance behavior has a mean score of 3.34 (SD=0.42) with a skew of 0.377 and kurtosis -1.348, and Technology has a mean score of 3.34 (SD=0.40) with a skew of -0.042 and kurtosis -0.383. Here, all variables show a normal data distribution as the statistical skewness and kurtosis are between -2 and +2.

In the statistical methodology of SEM-PLS, the size model must first be assessed before the structured model is evaluated. The main factor in determining the quality of the

size model is to assess the convergent and discriminant validity of the size model [26], [27].

TABLE II
DESCRIPTIVE STATISTICS

Variables	Average	SD	Min	Max	Tilt	Kurtosis
Misuse Prevention and Compliance	3.12	0.48	2.00	4.00	0.317	-0.640
Body of Knowledge	3.51	0.36	2.75	4.00	-0.219	-0.858
Skill	3.21	0.51	2.00	4.00	-0.105	-0.628
Behavioral Intervention	3.31	0.41	2.50	4.00	0.417	-0.897
Attitude	3.29	0.44	2.50	4.00	0.473	-0.902
Security Compliance Behavior	3.34	0.42	2.75	4.00	0.377	-1.348
Technology	3.34	0.40	2.25	4.00	-0.042	-0.383

SD= Standard deviation, Min=Minimal, Max=Maximum

Since the first-stage measure model shown in Fig. 2 is a fully bounced measure model, convergent validity assessment, criteria such as indicator loading, Cronbach Alpha (α) confidence, Composite confidence (ρ) and mean variance extracted (PVE)/AVE were used.

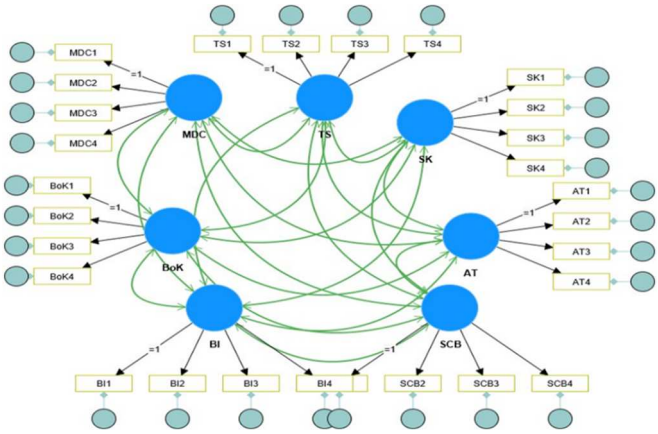

Fig. 2 Size Model Stage 1

2) Indicator Loading of the Measurement Framework:

The research framework was developed based on the literature review with theoretical background. Hence, confirmatory factor analysis (CFA) was considered a suitable approach for this research. CFA investigates whether the measured variables are consistent with our understanding of the variables and indicators in the research framework. Table 3 shows the indicator loading decision of the first size framework. This result shows several indicators that have loading values below the recommended threshold of 0.6 [28]. Therefore, all these indicators must be removed first to achieve unidimensionality for each construct.

TABLE III
MEASUREMENT FRAMEWORK INDICATOR LOADING (BEFORE CFA)

Latent Variables	Indicators	Loading
Attitude	Attitude 1	0.828
	Attitude 2	0.877
	Attitude 3	0.827
	Attitude 4	0.887
Behavioral Intervention	Behavioral Intervention 1	0.753
	Behavioral Intervention 2	0.858
	Behavioral Intervention 3*	0.582
	Behavioral Intervention 4	0.819
Body of Knowledge	Body of Knowledge 1	0.812
	Body of Knowledge 2	0.640
	Body of Knowledge 3	0.735
	Body of Knowledge 4	0.704
Misuse Prevention and Compliance	Misuse Prevention and Compliance 2 1	0.861
	Misuse Prevention and Compliance 2	0.857
	Misuse Prevention and Compliance 3	0.844
	Misuse Prevention and Compliance 4	0.840
Security Compliance Behavior	Security Compliance Behavior 1	0.917
	Security Compliance Behavior 2	0.830
	Security Compliance Behavior 3*	0.570
	Security Compliance Behavior 4	0.917
Skill	Skill 1	0.856
	Skill 2	0.697
	Skill 3	0.763
	Skill 4	0.845
Technology	Technology 1	0.761
	Technology 2	0.788
	Technology 3*	0.582
	Technology 4	0.750

The process of removing indicators that had loadings below the recommended 0.6. Three indicators were discarded in this process, i.e., Behavioral Intervention 3, Behavioral Security Compliance 3, and Technology 3. The loading values for each indicator were scrutinized each time the one item with the lowest loading value was removed. This process was repeated until the indicators that had loadings below 0.6 were removed. indicators with loadings below 0.6 were discarded because they did not have good multiple relationships with other indicators, as shown in Table 4.

TABLE IV
MEASUREMENT FRAMEWORK INDICATOR LOADINGS (AFTER CFA)

Latent Variables	Indicators	Loading
Attitude	Attitude 1	0.828
	Attitude 2	0.877
	Attitude 3	0.827
	Attitude 4	0.887
Behavioral Intervention	Behavioral Intervention 1	0.753
	Behavioral Intervention 2	0.858
	Behavioral Intervention 4	0.819
Body of Knowledge	Body of Knowledge 1	0.812
	Body of Knowledge 2	0.640
	Body of Knowledge 3	0.735
	Body of Knowledge 4	0.704
Misuse Prevention and Compliance	Misuse Prevention and Compliance 1	0.861
	Misuse Prevention and Compliance 2	0.857
	Misuse Prevention and Compliance 3	0.844
	Misuse Prevention and Compliance 4	0.840
Security Compliance Behavior	Security Compliance Behavior 1	0.917
	Security Compliance Behavior 2	0.830
	Security Compliance Behavior 4	0.917
Skill	Skill 1	0.856
	Skill 2	0.697
	Skill 3	0.763
	Skill 4	0.845
Technology	Technology 1	0.761
	Technology 2	0.788
	Technology 4	0.750

Cronbach Alpha (α) and Reliability Composite (ρ), with the decision of AVE

Table 5 shows the assessment results of two types of reliability, Cronbach Alpha (α) and composite reliability (ρ), with the AVE results for each embedded construct in the first rule assessment framework. Both reliability assessments show that all latent constructs have a good level of reliability, as the lowest value on the reliability composite is 0.828, and the Cronbach Alpha is 0.689. Therefore, it can be confirmed that the internal consistency of each construct is sufficient and can serve as evidence of the dimensionality of each construct [26], [27],[29].

TABLE V
COMPARISON OF PVE, COMPOSITE RELIABILITY AND CRONBACH ALPHA

	Construct	Before item removed			After item removed		
		AVE	ρ	α	AVE	ρ	α
1	Behavioral Intervention	0.578	0.843	0.750	0.700	0.875	0.785
2	Security Compliance Behavior	0.674	0.889	0.826	0.830	0.936	0.895
3	Technology	0.525	0.814	0.701	0.617	0.828	0.689

These three indicators have been removed by examining the impact on the convergent validity assessment (i.e., AVE/PVE = Average Extracted Variance), Composite Trustworthiness, and Cronbach Alpha. Behavioral Indicator Complying with Security 3 (Loading=0.570) was the first to be removed as it had the lowest loading value. These three indicators were necessary and helpful to remove from the analysis as they could all improve the convergent validity assessment (i.e., mean Explained Variance and Composite Reliability).

3) Fornell-Larcker

Table 6 shows the discriminant analysis results for the first stage assessment framework using the Fornell-Larcker criterion [30]. The power AVE values for each hidden construct have been calculated using this methodology. It was also used to compare the relationship values between the hidden constructs. According to the analysis, the power point value of AVE is greater than the outer factor of the borders. Therefore, it confirms that this first stage assessment framework has achieved discriminant even with no constructs accounting for the same thing, and the indicators accounting for each construct show a greater relationship than the relationship between the hidden variables.

TABLE VI
FORNELL-LARCKER DISCRIMINANT ASSESSMENT

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
(1)	**0.725**	0.00	0.00	0.00	0.00	0.00	0.00
(2)	0.527	**0.836**	0.00	0.00	0.00	0.00	0.00
(3)	0.311	0.519	**0.793**	0.00	0.00	0.00	0.00
(4)	0.351	0.505	0.521	**0.846**	0.00	0.00	0.00
(5)	0.425	0.531	0.440	0.494	**0.855**	0.00	0.00
(6)	0.375	0.472	0.514	0.545	0.612	**0.785**	0.00
(7)	0.488	0.529	0.463	0.539	0.684	0.535	**0.911**

Attention: Constructs; (1) =Body of Knowledge; (2)=Behavioral Interventions; (3)=Knowledge; (4)=Misuse Prevention and Compliance; (5)=Attitude; (6)=Technology; (7)=Security Compliance Behavior; AVE of each construct and element other than the bullet value is the value of the intermediate relationship between the constructs.

With this assessment, the discriminant state of the latent constructs holds when the loading levels of the target indicators to measure the respective latent constructs are higher loaded to the respective latent constructs compared to the latent construct balances [26], [27]. In conclusion, this discriminant assessment shows that indicator loadings are clearly different relative to the structure expressed in the theoretical framework. Hence, this study shows discriminant conditions for all hidden constructs; its findings agree with the results of the Fornell-Larcker discriminant analysis.

Table 7 shows the effect of independent constructs on the dependent constructs for the first stage of the measurement framework. For the first stage, the effect of the independent construct (Body of Knowledge and Technology) and its intermediate constructs (Behavioral security compliance, skills, attitude, and misuse prevention & Compliance) while the dependent construct (Attitude). The constructs used at this stage result from the measure framework obtained from the previous CFA (Confirmatory Factor Analysis) process.

TABLE VII
THE EFFECT OF INDEPENDENT CONSTRUCTS ON DEPENDENT CONSTRUCTS

Path	T Statistics
Body of Knowledge -> Skill	4.571
Body of Knowledge -> Misuse Prevention and Compliance	2.538
Body of Knowledge -> Attitude	3.925
Body of Knowledge -> Security Compliance Behavior	2.675
Behavioral Interventions -> Security Compliance Behavior	1.824
Skill -> Attitude	2.616
Misuse Prevention and Compliance -> Attitude	3.318
Attitude -> Behavioral Interventions	7.210
Attitude -> Security Compliance Behavior	6.794
Technology -> Misuse Prevention and Compliance	7.737

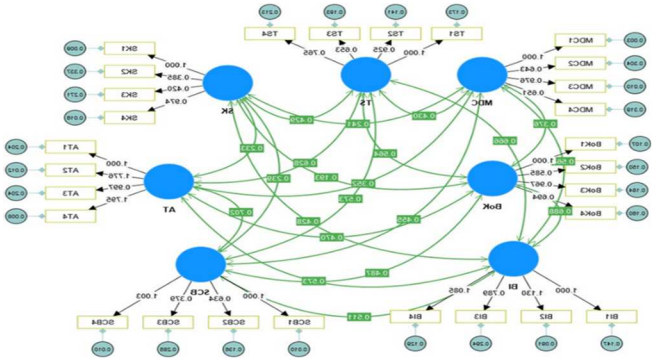

Fig. 3 Size Model stage 2

The significant effect of the independent construct on the dependent construct is identified through the t-statistic value. A t statistic value exceeding 1.96 indicates that the effect of an independent hidden variable on the dependent construct is significant. Ten paths have a significant effect, namely from the Knowledge Body construct to the proficiency construct, from the Knowledge Body construct to the Misuse Prevention and Compliance construct, from the Knowledge Body construct to the Attitude construct, from the Knowledge Body construct to the Security Behavior construct, from the Behavioral Intervention construct to the Behavior of Security Compliance, from the Proficiency construct to the Attitude construct, from the Misuse Prevention and Compliance construct to the Attitude construct, from the Attitude construct to the Behavioral Intervention construct, from the Attitude

construct to the Behavior of Security Compliance construct and from the Technology construct to the Misuse Prevention and Compliance construct. can be shown in Fig. 3.

B. Structured Framework Assessment

The main element discussed in this section is assessing a specific structured framework. As stated earlier, the valuation of structured trusses is based on various methodologies. These methodologies consist of determination pivot (R2), forecast multiplication (Q2), and size effect assessment (f2) for structured frames. This section also needs to assess the pass intervals of both structured frameworks. The following small section will discuss the assessment details of both structured frameworks.

1) Determination Percentage (R2), Forecast Percentage (Q2), and Impression Rating (f2):

In SEM-PLS investigations, most attention is paid to the explained variance of endogenous hidden constructs, which is measured through the use of estimating the covariance [27]. The exogenous hidden constructs each explain variation in the endogenous hidden constructs. This estimation shows the amount of this variation.

Referring to Table 8, the R2 value for the construct Security compliance behavior is 0.530. The value indicates that 5% of the total variation of this construct is explained by the three exogenous constructs (i.e., Attitude, Body of Knowledge, and Behavioral Interventions). In comparison, other factors explain the remaining 95% of the variation. The R2 for this endogenous construct has a moderate level of variation [31], [32], [26], [27], [33].

TABLE VIII
ASSESSMENT STRUCTURED FRAMEWORK R2

Endogenous VL	R^2	Note
Behavioral Interventions	0.282	Medium
Skill	0.097	Small
Misuse Prevention and Compliance	0.322	Medium
Attitude	0.346	Medium
Security Compliance Behavior	0.530	Large

In addition, the analysis also found that the variation in the endogenous constructs Behavioral Intervention, proficiency, Misuse prevention, and Attitude was explained by the exogenous construct Knowledge body at 28.2% (R2=0.282), 9.7% (R2=0.097), 32.2% (R2=0.322) and 34.6% (R2=0.346) respectively. Almost all of these values are moderate except proficiency at a low level. However, for the study of even better results, the R2 values need to be increased by future investigators. The value was improved by incorporating more variables into the framework studied and increasing the number of respondents studied.

As suggested by other principal investigators in the context of SEM-PLS, a Stone-Geisser (Q2) assessment was conducted to measure the overall predictive relevance of the endogenous hidden constructs in this Framework. However, this assessment is limited to the reflective endogenous latent constructs. The value of Q2 is zero. This means that each reflective construct in this framework, i.e., behavioral intervention constructs, skills, misuse prevention, and perspectives, have sufficient predictive linkage with their respective exogenous constructs. The Q2 assessment decision can be found in Table 9 [26].

Table 9 shows the detailed analysis of forecast linkage assessment for endogenous constructs with their respective exogenous constructs. The result of the analysis found that the Knowledge Body construct has a small relationship to the Behavioral Intervention construct (Q2=0.188), Proficiency (Q2=0.049), Misuse prevention and compliance (Q2=0.220), Attitude (Q2=0.247), and Security compliance behavior construct (Q2=0.427), In conclusion, the endogenous constructs in this framework can be predicted by their respective endogenous constructs as they have Q2 statistics that exceed zero [34]. Thus, this framework has sufficient forecasting power to predict the respective endogenous constructs [28].

TABLE IX
PREDICTIVE RELEVANCE OF ENDOGENOUS CONSTRUCTS

Endogenous VL	Q^2	Note
Behavioral Interventions	0.188	Medium
Skill	0.049	Small
Misuse Prevention and Compliance	0.220	Medium
Attitude	0.247	Medium
Security Compliance Behavior	0.427	Big

An equally important assessment in structured framework assessment is the effect size (f2) of exogenous constructs on endogenous constructs [26]. Table 10 shows that the construct Body of knowledge has a negligible effect on Proficiency (f2=0.107), Misuse Prevention and compliance (f2=0.037), Attitude (f2=0.086), and Security Compliant Behavior (f2=0.050). Next, the Proficiency construct has a negligible effect on Attitude (f2=0.046), Misuse Prevention and compliance (f2=0.093), the attitude construct has a significant effect on Intervention (f2=0.393), the Attitude construct has a medium effect on Use prevention and compliance (f2=0.294) and the Attitude construct has a significant effect on Security Compliant Behavior (f2=0.404). Finally, the technology construct has a medium effect on Misuse Prevention and compliance (f2=0.294).

TABLE X
EFFECT SIZE (F2) ENDOGENOUS CONSTRUCT OF A STRUCTURED FRAMEWORK

	f^2	Note
VL Endogenous: Skill VL Exogenous: Body of Knowledge	0.107	Small
VL Endogenous: Misuse Prevention and Compliance VL Exogenous: Body of Knowledge	0.037	Small
VL Endogenous: Skill VL Exogenous: Body of Knowledge	0.086	Small
VL Endogenous Security Compliance Behavior VL Exogenous: Body of Knowledge	0.050	Small
VL Endogenous: Attitude VL Exogenous: Skill	0.046	Small
VL Endogenous: Attitude VL Exogenous: Misuse Prevention and Compliance	0.093	Small
VL Endogenous: Behavioral Interventions VL Exogenous: Attitude	0.393	Large
VL Endogenous: Misuse Prevention and Compliance VL Exogenous: Attitude	0.294	Medium
VL Endogenous: Security Compliance Behavior VL Exogenous: Attitude	0.404	Large
VL Endogenous: Misuse Prevention and Compliance VL Exogenous: Technology	0.294	Medium

With the above three statistical analyses performed, the structured work-frame has met the minimum criteria for determining peptide (R2), forecast correlation (Q2), and

effect size (f2). Therefore, the structured framework proposed in Figure 4.8 can be assessed.

2) Path Coefficient Evaluation

Table 11 shows the results of the route multiplication in the proposed structured framework Fig. 4. The results show that all the routes, i.e. BoK → SK, BoK → MDC, BoK → AT, BoK → SCB, BI →SCB, SK → AT, MDC → AT, AT → BI, AT → SCB, TS →MDC have t values exceeding 1.96. Thus, all routes have significant effects from exogenous to endogenous constructs.

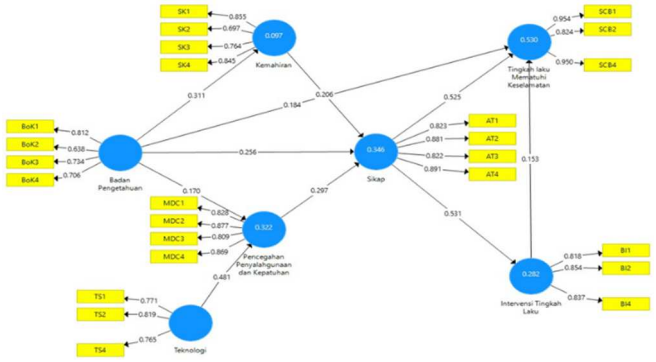

Fig. 4 Structured Framework Evaluation

TABLE XI
STRUCTURED FRAMEWORK OF PATH COEFFICIENTS

Path	PL	T-Value	P-Value	Result
BoK → SK	0.311	4.633	0.000	Significant
BoK→ MDC	0.353	5.338	0.000	Significant
BoK → AT	0.256	3.829	0.000	Significant
BoK → SCB	0.187	2.636	0.004	Significant
BI → SCB	0.159	1.777	0.038	Significant
SK → AT	0.206	2.632	0.004	Significant
MDC → AT	0.292	3.303	0.000	Significant
AT → BI	0.530	6.903	0.000	Significant
AT → SCB	0.518	6.592	0.000	Significant
TS →MDC	0.311	4.633	0.000	Significant

Attention: BoK=Knowledge Body; SK=Skills; MDC=Misuse Prevention and compliance; AT=Attitude; SCB=Security Behavior; BI=Behavioral Intervention; *Percentage is significant at 95% confidence level (*) if t-statistic >1.96 (p<0.05) and percentage is significant at 99% confidence level (**) if t-statistic >2.58 (p<0.01).

The analysis showed that the body of knowledge exerted significant (positive) on proficiency, misuse prevention & compliance, attitude, and security compliance behavior, respectively, with β=0.311, β=0.353, β=0.256, and β=.0.187. Behavioral interventions provided a significant (positive) effect on security compliance behaviors with β=0.159. Proficiency is significant (positive) on Attitude, i.e., β=0.206. Misuse prevention and compliance are significant (positive) to attitude, i.e., β=0.292. Attitude is significant (positive) to Behavioral intervention and Behavioral compliance, β=0.530 and β=0.518, respectively. Seterus Technology gives significant (positive) to the Prevention of misuse and compliance, i.e., β=0.311.

Therefore, it can be concluded that if the mean body of knowledge increases, then the mean proficiency, prevention of misuse & compliance, attitudes, and behaviors of complying with security will also increase. Similarly, if the mean score of Behavioral interventions increases, then the mean score of Security compliance behaviors will also increase. Furthermore, if the mean score of proficiency increases, the mean score of Attitude will also increase. Furthermore, if the mean score for misuse prevention and compliance increases, the mean score for attitude will also increase. Furthermore, if the mean score of Attitude increases, the mean score of Behavioral intervention and Security compliance behavior will also increase. Furthermore, if the mean score of technology increases, the mean score of Misuse prevention & compliance will also increase.

C. Assessment of Delivery Impression

In transmission analysis, the predominant researchers state that testing direct and indirect effects through the bootstrap route procedure, also known as bootstrap, is essential to confirm the existence of transmission effects [35]. This method is better stated than Baron and Kenny[36] method. As Hair et al. [26] suggested, the t-test procedure has been used to assess the indirect effects of the bootstrap procedure.

1) Testing Delivery Impressions:

The effects analysis aims to examine the intermediary effects between several proposed pathways. Table 12 shows the results of the indirect effects of mediation analysis for the structured framework. The results indicate that the indirect effect of the BoK→SK→BI pathway is significant (indirect effect coefficient = 0.135, t=3.072, p <0.05). Furthermore, the BoK→SK→AT pathway is significant (indirect effect coefficient = 0.103, t=2.638, p<0.05), the AT→BI→SCB pathway is significant (indirect effect coefficient = 0.132, t=3.184, p<0.05), and the BoK→AT→SCB pathway is significant (indirect effect coefficient = 0.151, t=2.760, p<0.05). Additionally, the BoK→SK→AT→SCB pathway is significant (indirect effect coefficient = 0.135, t=3.072, p<0.05), and the TS→MDC→AT→SCB pathway is significant (indirect effect coefficient = 0.154, t=2.734, p<0.05). These effects suggest that these indirect effects are important coefficients at the 99% confidence interval, as the observed t-value for these indirect effects is greater than the 99% critical t-statistic value (i.e., observed t-value > 2.58).

The following results indicate that the indirect effect of the SK→AT→BI pathway is significant (indirect effect coefficient = 0.112, t=2.264, p <0.05), and the BoK→SK→AT→BI pathway is significant (indirect effect coefficient = 0.035, t=2.033, p<0.05). Furthermore, the BoK→MDC→AT→BI pathway is significant (indirect effect coefficient = 0.154, t=2.734, p<0.05), the MDC→AT→BI pathway is significant (indirect effect coefficient = 0.055, t=2.176, p<0.05), and the TS→MDC→AT→BI pathway is significant (indirect effect coefficient = 0.065, t=2.376, p<0.05). Additionally, the MDC→AT→BI→SCB pathway is significant (indirect effect coefficient = 0.109, t=2.535, p<0.05), the SK→AT→SCB pathway is significant (indirect effect coefficient = 0.053, t=2.318, p<0.05), and the BoK→MDC→AT→SCB pathway is significant (indirect effect coefficient = 0.112, t=2.264, p<0.05). Furthermore, the MDC→AT→SCB pathway is significant (indirect effect coefficient = 0.035, t=2.033, p<0.05). These effects indicate that these indirect effects are important coefficients at the 95% confidence interval, as the observed t-value for these indirect effects is greater than the 95% critical t-statistic value (i.e., observed t-value > 1.96).

However, the analysis also shows that the indirect effect for the BoK→MDC→AT pathway is insignificant (indirect effect coefficient = 0.021, t=1.424, p>0.05). Additionally, the TS→MDC→AT pathway is not significant (indirect effect coefficient = 0.018, t=1.159, p>0.05), the BoK→AT→BI→SCB pathway is not significant (indirect effect coefficient = 0.005, t=1.071, p>0.05), and the SK→AT→BI→SCB pathway is not significant (indirect effect coefficient = 0.084, t=1.632, p>0.05). Furthermore, the BoK→SK→AT→BI→SCB pathway is not significant (indirect effect coefficient = 0.024, t=1.457, p>0.05), and the BoK→MDC→AT→BI→SCB pathway is not significant (indirect effect coefficient = 0.009, t=1.278, p>0.05). These effects are insignificant because the observed t-value for these indirect effects is less than the 95% critical t-statistic value (i.e., observed t-value < 1.96).

TABLE XII
ANALYZE THE INDIRECT EFFECTS OF THE STRUCTURED FRAMEWORK

Path Analysis	KTLP	T-Value	p-Value
BoK → SK → BI	0.135	3.072**	0.001
SK → AT → BI	0.112	2.264*	0.012
BoK → SK → AT →BI	0.035	2.033*	0.021
BoK → MDC → AT → BI	0.154	2.734*	0,003
MDC → AT → BI	0.055	2.176*	0.015
TS → MDC → AT → BI	0.065	2.376*	0.009
BoK → SK → AT	0.103	2.638**	0.004
BoK → MDC →AT	0.021	1.424	0.077
TS →MDC →AT	0.018	1.159	0.123
BoK →AT →BI →SCB	0.005	1.071	0.142
SK → AT → BI →SCB	0.084	1.632	0.051
BoK →SK → AT → BI →SCB	0.024	1.457	0.073
BoK → MDC → AT → BI →SCB	0.009	1.278	0.101
AT → BI →SCB	0.132	3.184**	0.001
MDC → AT → BI →SCB	0.109	2.535*	0.006
TS →MDC →AT →BI → SCB	0.034	2.306*	0.011
BoK → AT → SCB	0.151	2.760**	0.003
SK →AT → SCB	0.053	2.318*	0.010
BoK →SK →AT →SCB	0.135	3.072**	0.001
BoK →MDC →AT →SCB	0.112	2.264*	0.012
MDC →AT →SCB	0.035	2.033*	0.021
TS →MDC →AT → SCB	0.154	2.734**	0.003

Note: BoK = Body of Knowledge; SK = Skills; MDC = Misuse Prevention and Compliance; AT = Attitude; SCB = Security Compliance Behavior; BI = Behavioral Intervention; TS = Not Significant; KTLP = Indirect Effect Coefficient; a Coefficient is significant at the 95% confidence level (*) if t-statistic > 1.96 (p<0.05) and significant at the 99% confidence level () if t-statistic > 2.58 (p<0.01).**.

Equally important, a bootstrap confidence interval assessment for each indirect effect was also conducted and reported in the mediation effect test. Table 13 shows the results of the 95% bootstrap confidence interval. From the Table, it was found that the bootstrap confidence interval for these indirect effects includes zero for all types of bootstrap confidence interval analyses. Therefore, this confirms that mediation effects exist for the indirect coefficients. Evidence from this analysis indicates that the paths of indirect effects (Table 13) are consistent with the observed t-values of the indirect effects (Table 12).

TABLE XIII
BOOTSTRAP CONFIDENCE INTERVALS FOR INDIRECT EFFECTS STRUCTURED FRAMEWORK

Path Analysis KTLPa		95% Bootstrap Confidence Interval	
Path	(Indirect Effect Coefficient)	T-bootstrap	BCA-bootstrap
BoK → SK → AT	0.065*	(0.025, 0.118)	(0.020, 0.108)
Bok → MDC → AT	0.103*	(0.044, 0.174)	(0.043, 0.173)
BoK → AT →SCB	0.132*	(0.069, 0.201)	(0.073, 0.211)
AT→ BI →SCB	0.084*	(0.011, 0.172)	(0.009, 0.171)

Note: Partial Mediation; TS = Not Significant; KTLP = Indirect Effect Coefficient; a Path coefficient is significant at the 95% confidence level (*) if t-statistic > 1.96 (p<0.05) and significant at the 99% confidence level () if t-statistic > 2.58 (p<0.01).**.

In conclusion, it can be summarized that Skills (SK) mediate the correlation between Body of Knowledge (BoK) and Attitude (AT), as evidenced by the observed t-values and the 95% bootstrap confidence interval analysis of the indirect effect coefficients. Misuse Prevention (MDC) provides complete mediation in the correlation between Body of Knowledge (BoK) and Attitude (AT). Furthermore, Attitude (AT) also mediates the correlation between Skills (SK) and Security Compliance Behavior (SCB). Additionally, Behavioral Intervention (BI) mediates the correlation between Attitude (AT) and Security Compliance Behavior (SCB).

2) Classification of Mediation Effects

Through partial and full mediation concepts, this study uses procedures derived from the study by Zhao et al. [37] and aligns with the study by Baron and Kenny [36]. According to Hair et al. [28], if the indirect effect is significant, the research must determine whether the direct effect is significant to classify the construct as indirect only (full mediation), complementary mediation (partial mediation), or competitive mediation (partial mediation). Indirect-only mediation occurs if the direct effect is found to be insignificant. The research can differentiate between complementary and competitive mediation if the direct effect is significant. For the mediation effects in the second regulatory framework, as shown in Table 14.

TABLE XIV
BOOTSTRAP CONFIDENCE INTERVALS FOR INDIRECT EFFECTS STRUCTURED FRAMEWORK

Path	KTLP[a] (Indirect Effect Coefficient)	Path	PC[a] PL[a]	Types of Mediation
BoK → SK → AT	0.065*	BoK →AT	0.256	Partial Mediation
Bok → MDC → AT	0.103*	BoK→ AT	0.256	Partial Mediation
BoK → AT →SCB	0.132*	BoK → SCB	0.187	Partial Mediation
AT→ BI →SCB	0.084*	AT → SCB	0.518	Partial Mediation

Note: Partial Mediation; NS = Not Significant; ITCE = Indirect Effect Coefficient; PC = Path Coefficient; aPath coefficient is significant at the (*) confidence level if t-statistic > 1.96 (p < 0.05) and the coefficient is significant at the 99% confidence level (**) if t-statistic > 2.58 (p < 0.01).

It can be concluded that Skills (i.e., SK) provide partial mediation effects on the correlation between Body of Knowledge (i.e., BoK) and Attitude (i.e., AT). Misuse Prevention and Compliance (i.e., MDC) provide partial

mediation effects on the correlation between Body of Knowledge (i.e., BoK) and Attitude (i.e., AT). Attitude (i.e., AT) provides partial mediation effects on the correlation between Body of Knowledge (i.e., BoK) and Compliance Behavior (i.e., SCB). Behavioral Intervention (i.e., BI) provides partial mediation effects on the correlation between Attitude (i.e., AT) and Compliance Behavior (i.e., SCB).

D. Discussion of Findings

Table 15 shows the results of the indirect effect analysis for the third structural framework. The results indicate that the indirect effect of the BoK→SK→BI path is significant (indirect effect coefficient = 0.135, t = 3.072, p < 0.05). Similarly, the BoK→SK→AT path is significant (indirect effect coefficient = 0.103, t = 2.638, p < 0.05), as is the AT→BI→SCB path (indirect effect coefficient = 0.132, t = 3.184, p < 0.05). Additionally, the BoK→AT→SCB path is significant (indirect effect coefficient = 0.151, t = 2.760, p < 0.05), and the BoK→SK→AT→SCB path is significant (indirect effect coefficient = 0.135, t = 3.072, p < 0.05). Furthermore, the TS→MDC→AT→SCB path is significant (indirect effect coefficient = 0.154, t = 2.734, p < 0.05). These effects indicate that the indirect effects are significant at the 99% confidence interval because the observed t-values for these indirect effects are greater than 99% of the critical t-statistic values (i.e., observed t > 2.58).

The following results show that the indirect effect of the SK→AT→BI path is significant (indirect effect coefficient = 0.112, t = 2.264, p < 0.05). Similarly, the BoK→SK→AT→BI path is significant (indirect effect coefficient = 0.035, t = 2.033, p < 0.05), and the BoK→MDC→AT→BI path is significant (indirect effect coefficient = 0.154, t = 2.734, p < 0.05). The MDC→AT→BI path is also significant (indirect effect coefficient = 0.055, t = 2.176, p < 0.05), as is the TS→MDC→AT→BI path (indirect effect coefficient = 0.065, t = 2.376, p < 0.05). Additionally, the MDC→AT→BI→SCB path is significant (indirect effect coefficient = 0.109, t = 2.535, p < 0.05), and the SK→AT→SCB path is significant (indirect effect coefficient = 0.053, t = 2.318, p < 0.05). The BoK→MDC→AT→SCB path is significant (indirect effect coefficient = 0.112, t = 2.264, p < 0.05), and the MDC→AT→SCB path is significant (indirect effect coefficient = 0.035, t = 2.033, p < 0.05). These effects indicate that the indirect effects are significant at the 95% confidence interval because the observed t-values for these indirect effects are greater than 95% of the critical t-statistic values (i.e., observed t > 1.96).

However, the analysis also shows that the indirect effects for the BoK→MDC→AT path are not significant (indirect effect coefficient = 0.021, t = 1.424, p > 0.05). Similarly, the TS→MDC→AT path is not significant (indirect effect coefficient = 0.018, t = 1.159, p > 0.05). The BoK→AT→BI→SCB path is not significant (indirect effect coefficient = 0.005, t = 1.071, p > 0.05), and the SK→AT→BI→SCB path is not significant (indirect effect coefficient = 0.084, t = 1.632, p > 0.05). The BoK→SK→AT→BI→SCB path is not significant (indirect effect coefficient = 0.024, t = 1.457, p > 0.05), and the BoK→MDC→AT→BI→SCB path is not significant (indirect effect coefficient = 0.009, t = 1.278, p > 0.05). These are considered not significant because the observed t-values for these indirect effects are less than 95% of the critical t-statistic values (i.e., observed t < 1.96).

The response rate analysis indicates a rate of 86%. SEM-PLS analysis has demonstrated that the indicators used in this study possess a high ability to clarify the issues of interest. The evaluation criteria for SEM-PLS, including indicator loadings, Cronbach's Alpha (α), composite reliability (ρ), and Fornell-Larcker discriminant analysis, confirm that all indicators meet the minimum evaluation criteria. The measurement framework shows an acceptable level of capability for addressing the research phenomena of interest in this study.

The SEM-PLS path results show that an increase in the average level of Knowledge Body leads to an increase in the average level of Skills, Prevention of Misuse & Compliance, Attitudes, and Security Compliance Behavior. Similarly, an increase in the average level of Behavioral Intervention leads to an increase in the average level of Security Compliance Behavior. Furthermore, an increase in the average level of Skills leads to an increase in the average level of Attitudes. An increase in the average level of Prevention of Misuse and Compliance leads to an increase in the average level of Attitudes. An increase in the average level of Attitudes also leads to an increase in the average levels of Behavioral Intervention and Security Compliance Behavior. Additionally, an increase in the average level of Technology leads to an increase in the average level of Prevention of Misuse & Compliance.

Path coefficient assessments also show that the Knowledge Body has the largest contribution effect on Prevention of Misuse and Compliance, as the path coefficient value is the highest among the endogenous constructs from Knowledge Management Practices. Skills, Attitudes, and Security Compliance Behavior follow, ignoring negative and positive effects.

The analysis also indicates that the Knowledge Body has a significant (positive) effect on Skills, Prevention of Misuse & Compliance, Attitudes, and Security Compliance Behavior, respectively. Behavioral Intervention has a significant (positive) effect on Security Compliance Behavior. Skills have a significant (positive) effect on Attitudes. Prevention of Misuse and Compliance has a significant (positive) effect on Attitudes. Attitudes have a significant (positive) effect on both Behavioral Intervention and Security Compliance Behavior. Technology has a significant (positive) effect on Prevention of Misuse and Compliance, as the path coefficient value has a t-statistic above 1.96.

TABLE XV
SUMMARY OF CORRELATION HYPOTHESIS TEST RESULTS

Hypothesis	Result	Statistics Analysis
H1: There is a significant relationship between Knowledge and Attitude.	Support	PLS-SEM
H2: There is an important correlation between Knowledge and Skills.	Support	
H3: There is an important correlation between Knowledge Bodies and Misuse Prevention & Compliance.	Support	
H4: There is a significant correlation between Skills and Attitudes.	Support	
H5: There is a significant correlation between Misuse Prevention & Compliance and Attitude.	Support	

Hypothesis	Result	Statistics Analysis
H6: There is a significant correlation between Knowledge and Security Compliance Behavior.	Support	
H7: There is a significant correlation between Attitude and Security Compliance Behavior.	Support	
H8: There is a significant correlation between Attitude and Behavioral Intervention.	Support	
H9: There is a significant correlation between Behavioral Interventions and Security Compliance Behavior.	Support	
H10: There is a significant correlation between Technology and the Prevention of Misuse & Compliance.	Support	

It can also be concluded that Skills fully mediate the correlation between Knowledge Body and Attitudes. Prevention of Misuse and Compliance provides a full mediating effect on the correlation between Knowledge Body and Attitudes. Attitudes provide a full mediating effect on the correlation between Knowledge Body and Security Compliance Behavior. Behavioral Intervention provides a full mediating effect on the correlation between Attitudes and Security Compliance Behavior. The summary of the mediation hypothesis results is shown in Table 16.

TABLE XVI
SUMMARY OF MEDIATION HYPOTHESIS DECISION

Hypothesis	Result	The Impact of Mediation	Statistical Analysis
H11: The skill of mediating the correlation between Knowledge and Attitude.	Support	Partial Mediation	SEM-PLS
H12: Prevention of abuse & Compliance serves as an intermediary relationship between Knowledge and Attitude.	Support	Partial Mediation	
H13: Attitude serves as a mediator in the correlation between Knowledge and Safety Compliance Behavior.	Support	Partial Mediation	
H14: Behavioral interventions serve as a mediator in the correlation between attitudes and compliance with safety behaviors.	Support	Partial Mediation	

The analysis results show that all research questions have been answered and supported. This indicates that the determined factors have significant relationships overall. The relationships among these factors will be illustrated in the framework to be developed.

IV. CONCLUSION

The SEM-PLS path analysis results show that an increase in the average level of Knowledge Body leads to an increase in the average levels of Skills, Prevention of Misuse & Compliance, Attitudes, and Security Compliance Behavior. Similarly, an increase in the average level of Behavioral Intervention leads to an increase in the average level of Security Compliance Behavior. Furthermore, an increase in the average level of Skills leads to an increase in the average level of Attitudes. An increase in the average Prevention of Misuse and Compliance level also leads to an increase in the average level of Attitudes. Additionally, an increase in the average level of Attitudes leads to an increase in the average levels of Behavioral Intervention and Security Compliance Behavior. Moreover, an increase in the average level of Technology leads to an increase in the average level of Prevention of Misuse & Compliance.

This study is significant in helping university service employees understand the importance of maintaining information security. To enhance data validity, it is recommended that the study incorporate both qualitative and quantitative methods.

ACKNOWLEDGMENT

The authors thank the Yayasan Universitas Putra Indonesia "YPTK" Padang and Universiti Kebangsaan Malaysia for supporting this research.

REFERENCES

[1] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq, and M. K. Khan, "Comprehensive review of cybercrime detection techniques," *IEEE Access*, vol. 8, pp. 137293–137311, 2020, doi:10.1109/access.2020.3011259.

[2] Gushelmi, R. Latih, and A. M. Zin, "Level of User Security Behavior in the Service Industry," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 13, no. 4, pp. 1529–1536, 2023, doi: 10.18517/ijaseit.13.4.18425.

[3] J. Brands and J. Van Doorn, "The measurement, intensity and determinants of fear of cybercrime: A systematic review," *Comput. Human Behav.*, vol. 127, p. 107082, 2022, doi:10.1016/j.chb.2021.107082.

[4] A. Almansoori, M. Al-Emran, and K. Shaalan, "Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories," *Appl. Sci.*, vol. 13, no. 9, 2023, doi:10.3390/app13095700.

[5] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, "A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions," *ACM Comput. Surv.*, vol. 54, no. 11s, pp. 1–37, Jan. 2022, doi:10.1145/3514229.

[6] A. Chernikova *et al.*, "Cyber Network Resilience Against Self-Propagating Malware Attacks," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 13554 LNCS, no. 2019, pp. 531–550, 2022, doi: 10.1007/978-3-031-17140-6_26.

[7] S. Kamil, H. S. A. Siti Norul, A. Firdaus, and O. L. Usman, "The Rise of Ransomware: A Review of Attacks, Detection Techniques, and Future Challenges," in *2022 International Conference on Business Analytics for Technology and Security (ICBATS)*, IEEE, Feb. 2022, pp. 1–7. doi: 10.1109/icbats54253.2022.9759000.

[8] Y. Hong and S. Furnell, "Motivating Information Security Policy Compliance: Insights from Perceived Organizational Formalization," *J. Comput. Inf. Syst.*, vol. 62, no. 1, pp. 19–28, 2022, doi:10.1080/08874417.2019.1683781.

[9] A. Kovacevic, N. Putnik, and O. Toskovic, "Factors Related to Cyber Security Behavior," *IEEE Access*, vol. 8, pp. 125140–125148, 2020, doi: 10.1109/ACCESS.2020.3007867.

[10] L. Sanny, V. Angelina, and B. B. Christian, "Innovation of SME service industry in Indonesia in improving customer satisfaction," *J. Sci. Technol. Policy Manag.*, vol. 12, no. 2, pp. 351–370, Jan. 2021, doi: 10.1108/JSTPM-03-2020-0056.

[11] R. F. Ali, P. D. D. Dominic, S. Emad, A. Ali, and M. Rehman, "applied sciences Information Security Behavior and Information Security Policy Compliance : A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance," *Appl. Sci.*, 2021.

[12] I. Metin-Orta and D. Demirtepe-Saygılı, "Cyberloafing behaviors among university students: Their relationships with positive and negative affect," *Curr. Psychol.*, no. 0123456789, 2021, doi:10.1007/s12144-021-02374-3.

[13] S. Toker and M. H. Baturay, "Factors affecting cyberloafing in computer laboratory teaching settings," *Int. J. Educ. Technol. High. Educ.*, vol. 18, no. 1, 2021, doi: 10.1186/s41239-021-00250-5.

[14] S. Sugiyono, "Statitsika Untuk Penelitian," *Alfabeta Bandung*, vol. 12. pp. 1–415, 2007.
[15] J. D'Arcy and P. B. Lowry, "Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study," *Inf. Syst. J.*, vol. 29, no. 1, pp. 43–69, 2019, doi:10.1111/isj.12173.
[16] I. Alhassan, D. Sammon, and M. Daly, "Critical Success Factors for Data Governance: A Theory Building Approach," *Inf. Syst. Manag.*, vol. 36, no. 2, pp. 98–110, 2019, doi:10.1080/10580530.2019.1589670.
[17] I. Becker, "Measuring and understanding security behaviours," *PQDT - UK Irel.*, 2019.
[18] M. Butavicius, K. Parsons, M. Lillie, A. McCormac, M. Pattinson, and D. Calic, "When believing in technology leads to poor cyber security: Development of a trust in technical controls scale," *Comput. Secur.*, vol. 98, 2020, doi: 10.1016/j.cose.2020.102020.
[19] M. Choi and J. Song, "Social control through deterrence on the compliance with information security policy," *Soft Comput.*, vol. 22, no. 20, pp. 6765–6772, 2018, doi: 10.1007/s00500-018-3354-z.
[20] D. Bendler and M. Felderer, "Competency Models for Information Security and Cybersecurity Professionals: Analysis of Existing Work and a New Model," *ACM Trans. Comput. Educ.*, vol. 23, no. 2, 2023, doi: 10.1145/3573205.
[21] B. Alkhazi, M. Alshaikh, S. Alkhezi, and H. Labbaci, "Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior," *IEEE Access*, vol. 10, pp. 132132–132143, 2022, doi: 10.1109/ACCESS.2022.3230286.
[22] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Comput. Secur.*, vol. 31, no. 1, pp. 83–95, 2012, doi: 10.1016/j.cose.2011.10.007.
[23] F. H. S. Al Izki, "Exploring the Organisational, Social and Cultural Factors Influencing Those Employee Attitudes and Behaviours that Impact the Implementation of an Information Security Culture Within Omani Organisations," 2019.
[24] J. Deutrom, V. Katos, and R. Ali, "Loneliness, life satisfaction, problematic internet use and security behaviours: re-examining the relationships when working from home during COVID-19," *Behav. Inf. Technol.*, 2021, doi: 10.1080/0144929X.2021.1973107.
[25] C. C. Nwokeji, C. E. and Agubosim, "Effects of people's mental models of cybersecurity on their security behaviour," *Eur. J. Comput. Sci. Inf. Technol.*, vol. 10, no. 1, pp. 1–9, 2022, doi:10.37745/ejcsit/vol10.no1.pp1-9.
[26] J. F. Hair, M. Sarstedt, L. Hopkins, and V. G. Kuppelwieser, "Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research," *Eur. Bus. Rev.*, vol. 26, no. 2, pp. 106–121, 2014, doi: 10.1108/EBR-10-2013-0128.
[27] C. M. Ringle, M. Sarstedt, R. Schlittgen, and C. R. Taylor, "PLS path modeling and evolutionary segmentation," *J. Bus. Res.*, vol. 66, no. 9, pp. 1318–1324, 2013, doi: 10.1016/j.jbusres.2012.02.031.
[28] J. Hair, C. L. Hollingsworth, A. B. Randolph, and A. Y. L. Chong, "An updated and expanded assessment of PLS-SEM in information systems research," *Ind. Manag. Data Syst.*, vol. 117, no. 3, pp. 442–458, 2017, doi: 10.1108/IMDS-04-2016-0130.
[29] L. J. Cronbach, J. E. Deken, and N. Webb, "Research on Classrooms and Schools: Formulation of Questions, Design and Analysis.," *Occas. Pap. Eval. Consort.*, p. 243, 1976, [Online]. Available: https://eric.ed.gov/?id=ED135801
[30] C. Fornell and F. Larcker, David, "Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error.," *J. Mark. Res.*, vol. 18, no. 1, pp. 39–50, 1981.
[31] G. Cepeda-Carrión, J. F. Hair, C. M. Ringle, J. L. Roldán, and J. García-Fernández, "Guest editorial: Sports management research using partial least squares structural equation modeling (PLS-SEM)," *Int. J. Sport. Mark. Spons.*, vol. 23, no. 2, pp. 229–240, 2022, doi:10.1108/IJSMS-05-2022-242.
[32] C. Chang, "Relational bonds , customer engagement , and service quality," *Serv. Ind. J.*, vol. 41, no. 321, pp. 330–354, 2021.
[33] Chin W.W, "Chin1998," *MIS Quaterly*, vol. 22, no. 1. pp. vii–xvi, 1998.
[34] J. Henseler, "Partial least squares path modeling: Quo vadis?," *Qual. Quant.*, vol. 52, no. 1, pp. 1–8, 2018, doi: 10.1007/s11135-018-0689-6.
[35] K. J. Preacher and A. F. Hayes, "Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models," *Behav. Res. Methods*, vol. 40, no. 3, pp. 879–891, 2008, doi:10.3758/BRM.40.3.879.
[36] D. G. Kim and C. W. Lee, "Exploring the roles of self-efficacy and technical support in the relationship between techno-stress and counter-productivity," *Sustain.*, vol. 13, no. 8, pp. 1173–1182, 2021, doi: 10.3390/su13084349.
[37] X. Zhao, J. G. Lynch, and Q. Chen, "Reconsidering Baron and Kenny: Myths and truths about mediation analysis," *J. Consum. Res.*, vol. 37, no. 2, pp. 197–206, 2010, doi: 10.1086/651257.

Source details

International Journal on Informatics Visualization

Open Access

Years currently covered by Scopus: from 2017 to 2024

Publisher: Politeknik Negeri Padang

E-ISSN: 2549-9904

Subject area: Decision Sciences: Statistics, Probability and Uncertainty

Decision Sciences: Information Systems and Management

Computer Science: General Computer Science

Source type: Journal

CiteScore 2023
1.4

SJR 2023
0.211

SNIP 2023
0.403

View all documents > | Set document alert | Save to source list

CiteScore | CiteScore rank & trend | Scopus content coverage

CiteScore 2023

$$1.4 = \frac{630 \text{ Citations } 2020 - 2023}{441 \text{ Documents } 2020 - 2023}$$

Calculated on 05 May, 2024

CiteScoreTracker 2024

$$1.8 = \frac{1{,}036 \text{ Citations to date}}{574 \text{ Documents to date}}$$

Last updated on 05 December, 2024 • Updated monthly

CiteScore rank 2023

Category	Rank	Percentile
Decision Sciences — Statistics, Probability and Uncertainty	#114/168	32nd
Decision Sciences — Information Systems and	#106/148	28th

View CiteScore methodology > | CiteScore FAQ > | Add CiteScore to your site

About Scopus

What is Scopus

Content coverage

Scopus blog

Scopus API

Privacy matters

Language

日本語版を表示する

查看简体中文版本

查看繁體中文版本

Просмотр версии на русском языке

Customer Service

Help

Tutorials

Contact us

ELSEVIER

International Journal on Informatics Visualization • Volume 8, Issue 3-2, Pages 1976 - 1986 • 2024

Document type
Article

Source type
Journal

ISSN
25499904

DOI
10.62527/joiv.8.3-2.3094

Cybersecurity Behavior in the West Sumatra Universities

Gushelmi[a, b]; Latih, Rodziah[b] ; Zin, Abdullah Mohd.[c]
Save all to author list

[a] Faculty of Computer Science, Universitas Putra Indonesia YPTK, West Sumatra, Padang, Indonesia
[b] Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Selangor, Bangi, Malaysia
[c] Faculty of Computing and Multimedia, Universiti Poly-Tech Malaysia, Kuala Lumpur, Malaysia

Abstract

User cybersecurity behavior refers to the actions, habits, and decisions made by individuals when using technology and information that affect the level of security of the data and systems they access. Previous research has shown that user cybersecurity behavior is one of the leading causes of computer and information security issues in many organizations, particularly education. To address this issue, researchers must find solutions to improve user cybersecurity behavior within an organization. Therefore, this study aims to find the factors influencing user cybersecurity behavior in higher education institutions in West Sumatra in 2020. This study was conducted using a survey research method. A questionnaire was distributed to 155 respondents. The questionnaire consisted of 28 questions covering seven factors influencing user cybersecurity behavior. The survey data will be analyzed using the Structural Equation Model based on Partial Least Square. The research findings indicate that all variables, such as Misuse Prevention and Compliance, Body of Knowledge, Skill, Behavioral Intervention, Attitude, Security Compliance Behavior, and Technology, have significant relationships. The relationships between these factors will be shown in the framework to be developed. This indicates that the education sector in Indonesia is aware of cyber threats and the importance of security procedures in the workplace. For further research, a deeper exploration of

specific security issues is needed to propose potential solutions or actions that can be implemented to improve user cybersecurity behavior in the education sector, particularly in Indonesia.

Author keywords

behavior; universities; User cybersecurity

SciVal Topics

Funding details

References (37)

View in search results format >

All

Export Print E-mail Save to PDF Create bibliography

1 Al-Khater, W.A., Al-Maadeed, S., Ahmed, A.A., Sadiq, A.S., Khan, M.K.

Comprehensive review of cybercrime detection techniques

(2020) *IEEE Access*, 8, art. no. 9146148, pp. 137293-137311. Cited 83 times.
http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6287639
doi: 10.1109/ACCESS.2020.3011259

View at Publisher

2 Gushelmi, Latih, R., Zin, A.M.

Level of User Security Behavior in the Service Industry

(2023) *International Journal on Advanced Science, Engineering and Information Technology*, 13 (4), pp. 1529-1536.
ijaseit.insightsociety.org
doi: 10.18517/ijaseit.13.4.18425

View at Publisher

3 Brands, J., Van Doorn, J.

The measurement, intensity and determinants of fear of cybercrime: A systematic review

(2022) *Computers in Human Behavior*, 127, art. no. 107082. Cited 22 times.
https://www.journals.elsevier-com.uptm.remotexs.co/computers-in-human-behavior
doi: 10.1016/j.chb.2021.107082

View at Publisher

4 Almansoori, A., Al-Emran, M., Shaalan, K.

Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories

(2023) *Applied Sciences (Switzerland)*, 13 (9), art. no. 5700. Cited 24 times.
www.mdpi.com/journal/applsci/
doi: 10.3390/app13095700

View at Publisher

About Scopus

What is Scopus

Content coverage

Scopus blog

Scopus API

Privacy matters

Language

日本語版を表示する

查看简体中文版本

查看繁體中文版本

Просмотр версии на русском языке

Customer Service

Help

Tutorials

Contact us