Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 4, August 2025, Page. 1897-1910
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4861

Quantitative Analysis of the Key Factors Driving Cybersecurity Awareness Among Information Systems Users

Muhammad Agreindra Helmiawan[1], Esa Firmansyah[2], Dody Herdiana[3], Yopi Hidayatul Akbar[4], A'ang Subiyakto[5], Titik Khawa Abdul Rahman*[6]

[1,2,3,4]Informatics, Faculty of Information Technology, Sebelas April University, Sumedang, Indonesia
[5]Information System, Faculty of Science and Technology, Syarif Hidayatullah State Islamic University, Jakarta, Indonesia
[6]Information and Communication Technology, Asia e University, Subang Jaya, Malaysia

Email: [6]titik.khawa@aeu.edu.my

Received : Jun 11, 2025; Revised : Jul 18, 2025; Accepted : Aug 16, 2025; Published : Aug 18, 2025

Abstract

Cybersecurity threats are increasingly complex and widespread, posing significant risks to individuals and organizations. However, many studies tend to address the technological or behavioral aspects separately. The study uses a survey-based quantitative approach using PLS-SEM to analyze key factors that influence cybersecurity awareness, including demographics, training, psychological bias, and organizational culture. The findings suggest that several constructs-such as threat awareness, perceived risk, and education-significantly predict cybersecurity awareness and behaviour. Notably, the model yields an R^2 value of up to 0.703 with a strong path significance ($p < 0.05$), which underscores the robustness of the relationship. This study offers an integrated perspective on cybersecurity by bridging the psychological, educational, and organizational dimensions. It highlights cybersecurity awareness as a mediating construct that links upstream factors to secure user behavior-a relational structure that has not been explored in previous research.

Keywords : *Cybersecurity Awareness, Digital Resilience, Organizational Policies, Risk Perception, User Behaviour*

1. INTRODUCTION

In the contemporary digital era, the importance of cybersecurity awareness among information system users has risen to a critical level [1]. As digital connectivity becomes ubiquitous across various sectors, the potential for cyber threats to compromise organisational assets, personal information, and national security has correspondingly increased [2], [3]. These threats are characterised not only by their rising frequency but also by their escalating sophistication and the potential for severe consequences, which necessitates a comprehensive understanding of the underlying human and organisational factors that influence cybersecurity practices [4].

Organisations and governmental agencies are thus compelled to confront a rapidly evolving threat landscape, one that demands the cultivation of a resilient cybersecurity culture [5]. Such a culture must extend beyond traditional technological safeguards to encompass behavioural change, organisational policies, and the fostering of proactive security practices [6], [7]. This holistic perspective recognises that technological solutions alone are insufficient; rather, the human element plays an equally pivotal role in the effectiveness of cybersecurity measures[8], [9].

The relationship between human factors and technological safeguards is complex and multifaceted, requiring careful consideration of organisational culture, training initiatives, and user empowerment [10], [11], [12]. These elements collectively contribute to a security-conscious environment where individuals are not only aware of potential threats but are also motivated and equipped to act by security best practices [13], [14], [15]. By delving into the core drivers of

Vol. 6, No. 4, August 2025, Page. 1897-1910
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4861

cybersecurity awareness, organisations can better understand how to support their personnel in developing the requisite knowledge, skills, and attitudes to navigate the intricacies of the cyber terrain effectively [16].

Unlike previous studies, which often focus predominantly on either technological solutions or behavioural interventions in isolation, this research seeks to explore the integrative nature of these factors within organisational contexts. It aims to address existing gaps by examining how human and technological elements interact and influence each other in fostering a robust security culture. This expanded focus is intended to provide a more nuanced understanding of the mechanisms that underpin effective cybersecurity practices.

The overarching objective of this research is to systematically identify and analyse the organisational, behavioural, and technological determinants that influence cybersecurity awareness among users of information systems. Through a comprehensive investigation, the study aims to generate insights that can inform the development of effective strategies for cultivating a security-conscious culture. Such strategies are anticipated to enhance organisational resilience, reduce the likelihood of security breaches, and contribute to the broader goal of safeguarding digital assets in an increasingly volatile cyber environment.

2. METHOD

2.1. Research Design

This study uses quantitative research methodology to investigate the factors that influence the utilisation of information systems. This approach has been chosen to facilitate the collection and analysis of objective and systematic empirical data, as well as the collection of data from a randomly selected sample of participants simultaneously. The research stages are divided into three stages, as illustrated in Figure 1, followed by a description of each stage.

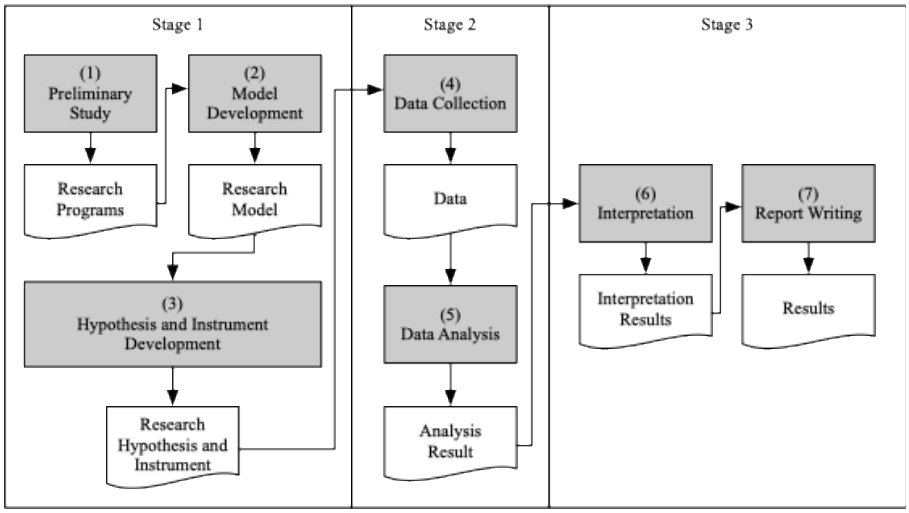

Figure 1. Research Procedure

The research procedure begins with an initial phase that encompasses a preliminary study, during which existing literature and prior research are thoroughly reviewed to identify gaps and establish a foundational understanding. This stage sets the groundwork for subsequent development. Following this, the model development process is undertaken, involving the design and refinement of theoretical frameworks or conceptual models pertinent to the research objectives. Subsequently, hypotheses are formulated, and appropriate instruments or tools for data collection are meticulously developed to ensure they are valid and reliable.

The second stage begins with the systematic collection of data, employing the instruments crafted during the initial phase. This process involves careful planning to ensure that data is gathered ethically

Vol. 6, No. 4, August 2025, Page. 1897-1910
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4861

and accurately, adhering to the established research design. Once the data have been collected, they undergo rigorous analysis employing suitable statistical or qualitative methods, depending on the nature of the data and the research questions.

The final stage involves interpreting the analysed data, where the findings are examined about the original hypotheses and research objectives. This phase is crucial for deriving meaningful conclusions and insights. Subsequently, a comprehensive research report is compiled, documenting the methodology, findings, interpretations, and implications of the study. This report aims to contribute to the existing body of knowledge and provide a foundation for future research endeavours.

2.2. Participant and Sampling

Surveys were distributed to a diverse group of participants to collect data, ensuring representation across various demographic variables, including age, gender, educational level, and professional background. The sample size was established through statistical power analysis to guarantee adequate statistical power for detecting significant relationships among the variables of interest.

2.3. Data Collection

The process of data collection involves administering structured questionnaires to participants through online platforms. The instrument utilised for the questionnaire was developed following a comprehensive review of the existing literature and validated scales to ensure both content validity and reliability. Furthermore, the questionnaire underwent pre-testing with a select group of individuals to enhance clarity and comprehension. The data collected through the questionnaire encompassed various dimensions of cybersecurity awareness, including knowledge of security threats, attitudes towards security practices, perceived self-efficacy in implementing security measures, and engagement in secure behaviours. Demographic information was also gathered to account for potential confounding variables.

The explicit model for measuring constructs involves a systematic and detailed approach to assessing the reliability and validity of research instruments. The initial step is calculating convergent reliability, which aims to ensure that the indicators within the construct are positively and strongly correlated with each other. This calculation is typically conducted using Cronbach's Alpha coefficient, with the formula:

$$\alpha = \left(\frac{k}{(k-1)}\right) * \left(1 - \frac{\Sigma\sigma i^2}{\sigma t^2}\right) \quad (1)$$

Where (k) is the number of indicators, $\Sigma\sigma i^2$ is the variance of the ith indicator, and σt^2 is the variance of the total score.

Subsequently, construct validity analysis is performed, including convergent and discriminant validity. Convergent validity is examined through the Average Variance Extracted (AVE), calculated with the formula:

$$AVE = \left(\sum \lambda i^2\right)/n \quad (2)$$

Where λi is the factor loading of indicator (i). The AVE value must be at least 0.50, indicating that the indicators can explain at least half of the construct's variance. Discriminant validity is assessed by comparing the AVE with the correlations between constructs, which are calculated using the Pearson correlation coefficient (r) and tested for significance.

The final stage involves measuring the predictive power of the construct, which is conducted through regression analysis with the formula:

Vol. 6, No. 4, August 2025, Page. 1897-1910
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4861

$$R^2 = 1 - \frac{SS_{residual}}{SS_{total}} \quad (3)$$

where R^2 Indicates the proportion of variance in the dependent variable explained by the construct, $SS_{residual}$ is the residual sum of squares, and SS_{total} the total sum of squares. The regression coefficient is also analysed to evaluate the strength and significance of the prediction.

Overall, this explicit model provides a comprehensive and detailed overview of the reliability, validity, and predictive power of the construct, which are crucial foundations for decision-making and further research development.

2.4. Research Hypothesis

This study employed a research model to investigate the relationships among variables recognised as critical factors affecting cybersecurity, as demonstrated in Figure 2. The hypotheses derived from previous discussions informed the analysis of these relationships within the proposed model. Numerous studies have indicated that age may significantly influence an individual's awareness of security risks [17].

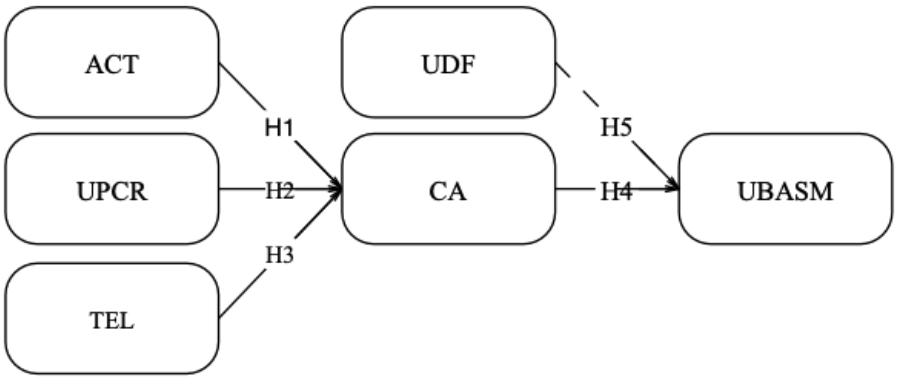

Figure 2. Research Hypothesis

H1: Awareness of Cybersecurity Threats (ACT) significantly increases users' Cybersecurity Awareness (CA).

H2: User Perceptions of Cybersecurity Risks (UPCR) positively influence Cybersecurity Awareness (CA).

H3: The Level of Training and Education (TEL) significantly enhances users' cybersecurity awareness (CA).

H4: Cybersecurity Awareness (CA) significantly and positively impacts User Behaviour in Adopting and complying with Security Measures and best practices (UBASM).

H5: User Demographic Factors (UDF) significantly moderate the relationship between cybersecurity awareness and user security behaviour.

Cybersecurity knowledge is very important in determining someone's awareness of internet safety [18], [19]. How people perceive cybersecurity can also significantly impact their level of understanding. It is important to consider the demographic variations in awareness, particularly between genders, as highlighted by previous research [19], [20], [21]. Young people have been found to lack proper security precautions when using the internet; older individuals may also struggle to understand cybersecurity practices [1], [22], [23], [24]. Cybersecurity awareness training programs have shown that providing training to older individuals enhances their cybersecurity abilities.

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 4, August 2025, Page. 1897-1910
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4861

3. RESULT

The results of this study provide valuable insights into the factors that influence cybersecurity awareness among users of information systems. The collected data will be analysed utilising descriptive statistics, correlation analysis, and regression analysis to yield a comprehensive understanding of the key factors that influence cybersecurity awareness.

3.1. Descriptive Statistics

The descriptive analysis summarised the characteristics of the sample and the distribution of the variables under investigation. Frequencies, percentages, means, and standard deviations were calculated for demographic factors, levels of awareness, perceptions of risk, training and education, and security behaviours. The relationship between the research variables used and their processing using PLS-SEM is presented in Figure 3, followed by an explanation of the process, analysis, and results of this research. The analysis focused on 254 participants located in West Java, Indonesia. Additionally, the validity and reliability of the constructs were thoroughly evaluated. The validity was assessed using the Average Variance Extracted method, while the reliability was determined through Composite Reliability and Cronbach's Alpha.

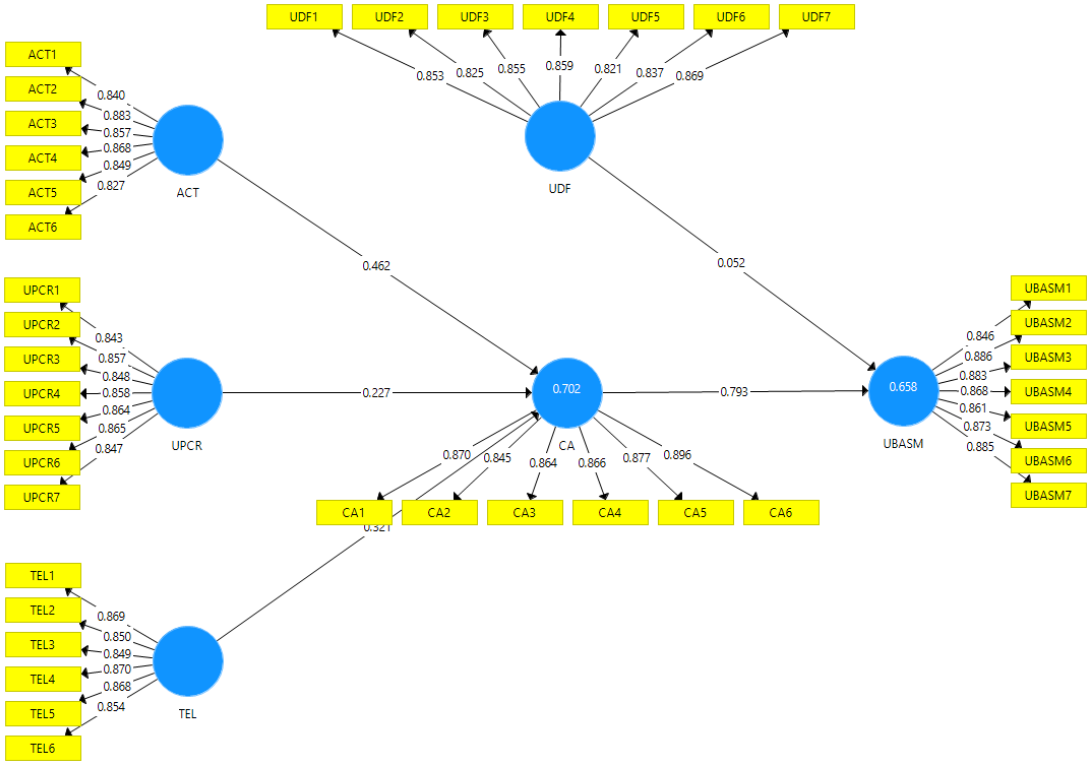

Figure 3. Relationship Between Research Variables

The results of the convergence reliability and validity analysis for each construct used in the research model are shown in Table 1. This includes values for Cronbach's Alpha, Rho_A, Composite Reliability (CR), and Average Variance Extracted (AVE). The purpose of this evaluation is to ensure that the indicators within each construct can consistently and validly represent their respective constructs. The Cronbach's Alpha values for all constructs exceed the minimum threshold of 0.70, indicating that the internal reliability of each construct falls within a satisfactory category. Notably, the UBASM construct achieved the highest score (0.947), followed closely by CA (0.936), demonstrating a very strong consistency in the respondents' answers regarding the items within these constructs. The

Vol. 6, No. 4, August 2025, Page. 1897-1910
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4861

ACT construct yielded the lowest Cronbach's Alpha value (0.926), although it remains within acceptable limits. Moreover, the Rho _ A value, which serves as a more precise estimator of reliability in the context of PLS-SEM, also exhibits satisfactory results, with all values surpassing the threshold of 0.70. This signifies that the constructs in the model possess high structural stability. The CR value further corroborates that the overall construct demonstrates excellent combined reliability, with values ranging from 0.942 to 0.957. These figures significantly exceed the minimum threshold of 0.70, indicating that the overall indicators within each construct consistently measure the latent variable in question.

Regarding the AVE, all constructs report values exceeding the minimum limit of 0.50, signifying that more than 50% of the variance in the indicators can be explained by the respective constructs being measured. The highest AVE value was recorded in the UBASM construct (0.760), and the lowest value was recorded in the UDF construct (0.715). Overall, the test results indicate that the entire construct within the model exhibits commendable reliability and convergent validity, rendering it suitable for advanced structural analysis within the context of PLS-SEM.

Table 1. Convergent Reliability & Validity

No	Construct	Cronbach's Alpha	rho_A	Composite Reliability	AVE
1	ACT	0.926	0.927	0.942	0.729
2	CA	0.936	0.936	0.949	0.757
3	TEL	0.930	0.931	0.945	0.739
4	UBASM	0.947	0.948	0.957	0.760
5	UDF	0.934	0.935	0.946	0.715
6	UPCR	0.938	0.940	0.950	0.730

The discriminant validity, as shown in Table 2, assesses the degree to which a construct within the model can empirically differentiate itself from another construct. One methodology employed to measure discriminant validity is the Fornell-Larcker criterion, which posits that the square root of the Average Variance Extracted (AVE) for each construct should exceed the correlation between that construct and the other constructs. The table indicates that all the diagonal values, highlighted in bold, which represent the square root values of the AVE, surpass the correlation values among the other constructs.

Table 2. Discriminatory Validity

No	Construct	ACT	CA	TEL	UBASM	UDF	UPCR
1	ACT	**0.854**					
2	CA	0.751	**0.870**				
3	TEL	0.490	0.651	**0.860**			
4	UBASM	0.523	0.810	0.503	**0.872**		
5	UDF	0.327	0.321	0.207	0.307	**0.846**	
6	UPCR	0.579	0.641	0.455	0.558	0.247	**0.854**

For instance, the ACT construct has a square root of the average variance extracted (AVE) of 0.854, which surpasses its correlations with other constructs, including CA (0.751), TEL (0.490), UBASM (0.532), UDF (0.327), and UPCR (0.579). This pattern is similarly observed in the UPCR construct, which has an AVE value of 0.854, exceeding its correlation with ACT (0.579), CA (0.641), TEL (0.455), UBASM (0.588), and UDF (0.247). The UBASM construct demonstrates exceptional discriminant validity, with a square root AVE value of 0.872, which is markedly higher than all other correlation values associated with the construct. Even the construct with the highest correlation to UBASM, namely CA (0.810), remains below its AVE value. Concurrently, the UDF construct exhibits

Vol. 6, No. 4, August 2025, Page. 1897-1910
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4861

an AVE square root value of 0.846, which also surpasses its correlation with other constructs, such as CA (0.321) and UBASM (0.307), indicating that although the moderating contribution of the UDF is relatively minor, it still meets the criteria for discriminant validity. Collectively, these findings imply that each construct within the model demonstrates adequate discriminant validity, as it accounts for a greater variance from its indicators than the variance shared with other constructs. This substantiates that the constructs employed in the model are conceptually and empirically distinctive from each other, allowing for their independent utilisation in advanced studies analysis.

The R^2 (R-Squared) and R^2 Adjusted values for endogenous constructs in structural models, CA and UBASM, are presented in Table 3. These two indicators are used to evaluate the model's predictive ability for dependent or endogenous variables. The construct CA has an R^2 value of 0.703 and an Adjusted R^2 value of 0.698. This means that as much as 62.1% of the variance in the CA construct can be explained by the exogenous constructs, i.e. ACT, UPCR, and TEL. These values are categorised as quite strong according to the interpretation guidelines, which state that R^2 values are considered weak (0.25), moderate (0.50), and strong (0.75). An Adjusted R^2 value that is only slightly lower than R^2 indicates the consistency and stability of the model, especially after considering the number of predictors in the model. The UBASM construct shows an R^2 value of 0.658 and an Adjusted R^2 of 0.656, indicating that 53.9% of the variance in UBASM can be explained by the CA construct. It also falls under the category of medium predictive power. The Adjusted R^2 value, which is close to the R^2 value, again reinforces the evidence that the model exhibits good predictive stability, without overfitting or significant multicollinearity effects. Overall, these results suggest that the model has sufficient predictive capabilities to explain changes in the main endogenous construct. The high R^2 and R^2 Adjusted values confirm that the exogenous constructs incorporated into the model successfully predict user behaviour and awareness of cybersecurity with significant accuracy.

Table 3. R Square

No	Endogenous constructs	R^2	R^2 Adjusted
1	CA	0.703	0.698
2	UBASM	0.658	0.656

3.2. Hypothesis Testing

The study's findings substantiate the analysis of the correlation and level of significance between the independent variable and the dependent variable. Table 4 delineates the outcomes of hypothesis testing, which aims to evaluate the robustness of the relationship between constructs within the research model through the Path Coefficient (β), t-statistic, and p-value.

Table 4. Path Coefficients

No	Hypothesis	Cronbach's Alpha	Original Sample	Sample Mean	Standard Deviation	t-Statistics	p-Values	Results
1	H1	ACT → CA	0.462	0.463	0.044	10.602	0.000	Sig
2	H2	CA → UBASM	0.793	0.792	0.025	31.363	0.000	Sig
3	H3	TEL → CA	0.321	0.322	0.041	7.809	0.000	Sig
4	H4	UDF → UBASM	0.052	0.057	0.035	1.518	0.130	No
5	H5	CA × UDF → UBASM	0.227	0.227	0.0043	5.341	0.000	Sig

Vol. 6, No. 4, August 2025, Page. 1897-1910
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4861

From this table, it can be seen that H1 (ACT→CA) has a positive path coefficient of 0.462, with a statistical t-value of 10.602 and a p-value of 0.000, indicating a significant relationship between the ACT and CA variables. Similarly, H2 (CA→UBASM) showed a strong and positive relationship, with a path coefficient of 0.793, a t-statistic of 31.363, and a p-value of 0.000, indicating that the relationship between the CA and UBASM variables was also significant. The H3 hypothesis (TEL→CA) also showed a positive and significant relationship with a path coefficient of 0.321, a t-statistic of 7.809, and a p-value of 0.000. This means that the TEL variable has a considerable influence on CA. Finally, H5 (CA × UDF→UBASM), which may represent the interaction effect, showed a path coefficient of 0.227, a t-statistic of 5.341, and a p-value of 0.000, indicating that the effect of interaction between CA and UDF on UBASM was significant. In contrast, the H4 hypothesis (UDF→UBASM) has a very low path coefficient of 0.052, with a t-statistic of 1.518 and a p-value of 0.130. Since the p-value (0.130) is greater than the general significance threshold (usually 0.05), the relationship between the UDF and UBASM variables is insignificant. This means that the data do not support the significant influence of UDF on UBASM in this model.

Overall, most of the hypotheses in this study (H1, H2, H3, and H5) are supported by the data, indicating a significant relationship between the variables, except for H4, where the relationship between the UDF and UBASM variables is not important.

Table 5 presents the effect size value (f^2) utilised to assess the magnitude of the influence of each exogenous construct on the endogenous construct within a structural model. This f^2 value offers supplementary insights beyond the R^2 value, specifically regarding the extent to which a construct contributes to the augmentation of the R^2 value of the dependent construct, contingent upon whether the construct is integrated or excluded from the model.

Table 5. Assessing the Influence Strength of Constructs

No	Relationship	f^2	Strength
1	ACT → CA	0.430	Medium
2	CA → UBASM	1.651	Large
3	TEL → CA	0.247	Small
4	UDF → UBASM	0.007	Small
5	UPCR → CA	0.109	Medium

The results of the analysis showed variations in the strength of influence between the constructs, and the relationship between ACT and CA (ACT→CA) resulted in an f^2 value of 0.430, which was categorised as a Medium influence. This indicates that the ACT construct makes a moderate contribution to explaining the variance in the CA construct. In the relationship between CA and UBASM (CA→UBASM), the value of f^2 reaches 1.651. This value is classified as very high and is considered to have a large influence. These findings show that the CA construct has a dominant and significant role in explaining the variance in the UBASM construct. For the relationship between TEL and CA (TEL→CA), the value of f^2 is 0.247, which is categorised as a Minor influence. This suggests that TEL's contribution to explaining variance in CA is relatively limited. The relationship between UDF and UBASM (UDF → UBASM) showed the lowest f^2 value, which was 0.007. This value is also classified as Small, indicating that the UDF makes a very minimal or negligible contribution to the variance in UBASM. Finally, the relationship of UPCR and CA (UPCR→CA) results in an f^2 value of 0.109, which is categorised as a Medium influence. This suggests that UPCR has a moderate contribution in explaining variance in CA.

Overall, the influence strength analysis revealed that the CA construct had the most substantial and strongest influence on UBASM. At the same time, the other variables exhibited influence strengths

that varied from medium to small. These findings provide important insights into the relative significance of each relationship in the hypothetical model.

Table 6 presents the results of the analysis of specific indirect effects in structural models, which crucially test the mediation hypothesis through the CA construct (as a mediator). This data includes three hypothesised mediation pathways: ACT → CA → UBASM, TEL → CA → UBASM, and UPCR → CA → UBASM. For each track, the t-statistics and p-values are presented as indicators of statistical significance. Results showed that all mediating pathways consistently had a p-value of 0.000, which is substantially smaller than the conventional significance level ($p < 0.05$). This consistency emphatically indicates that the indirect effects of ACT, TEL, and UPCR on CA-mediated UBASM are statistically significant. These findings provide strong empirical support for the role of CA mediation, confirming that the influence of independent variables (ACT, TEL, UPCR) on dependent variables (UBASM) is largely or entirely explained through the intermediate pathway of CA. Thus, CA serves as a key mechanism that transmits the influence of antecedent constructs to UBASM.

Table 6. Spesific Indirect Effect

No	Relationship	t-Statistics	p-Values
1	ACT → CA → UBASM	10.514	0.000
2	TEL → CA → UBASM	7.338	0.000
3	UPCR → CA → UBASM	5.211	0.000

The results of the construct effect measurement indicate that CA fulfils a pivotal role in mediating the influence of antecedent factors on UBASM. While several other exogenous variables exert a moderate to minor influence, this highlights the necessity for strategic interventions aimed at enhancing user awareness of digital security and improving security behaviour within the online environment. This study enhances the existing body of knowledge by identifying crucial elements that influence individuals' cybersecurity behaviour. The results underscore the importance of improving cybersecurity education by customising it to address specific knowledge gaps and psychological factors [25]. The findings highlight the necessity for comprehensive strategies that consider both cognitive and affective aspects of cybersecurity awareness to encourage responsible online behaviour. The Anti-Phishing Working Group reported numerous unique phishing websites during the first quarter of 2016, illustrating the persistent and evolving nature of cyber threats [1]. Phishing susceptibility is affected by various factors, including the context of the email, prior experiences with phishing attacks, and individual impulsivity [26]. A study conducted at a large public university involved sending emails to staff members containing a link to a study website. The results indicated that many users clicked on the link, emphasising the need for enhanced awareness and training regarding susceptibility to phishing. The findings suggest that various factors, including individual differences in cognitive abilities, personality traits, and risk perception, influence susceptibility to phishing. Additionally, habits play a role in phishing susceptibility; individuals who engage in email-related tasks automatically may exhibit less suspicion and, consequently, be more vulnerable to phishing attacks [27]. When individuals evaluate emails and follow web browser warnings, they employ various tactics with varying levels of effectiveness.

Furthermore, individuals may be susceptible to phishing scams due to a lack of awareness regarding the associated risks, an absence of self-perceived vulnerability, or inadequate practical strategies for identifying phishing emails [28]. Users' susceptibility to phishing may also be influenced by numerous factors, including their educational background, knowledge, and experience [28]. Moreover, a person‘s behaviour may depend on their evaluation of potential outcomes, underscoring the importance of understanding individuals' risk perceptions and decision-making processes. It has also been demonstrated that the behaviour of those who click on links may be motivated by a desire to

perform well in their professional roles [28]. Additionally, a study identified characteristics that affect susceptibility to social media phishing attempts, concluding that certain individuals are more vulnerable due to their online behaviour, cognitive processing, demographics, knowledge of information and communication technology, and personality traits. There are few organised classifications of variables influencing phishing susceptibility, indicating that further research in this domain is essential.

4. DISCUSSIONS

The outcomes of this study provide invaluable insights into the factors that influence users' cybersecurity awareness in information systems. The study's conclusions carry significant implications for the development of effective cybersecurity awareness programs and interventions, despite being grounded in the specific context of the study sample.

Firstly, this study emphasises the need to tailor cybersecurity awareness initiatives to specific demographic groups. Education and tailored messaging can effectively address knowledge gaps and biases, thereby enhancing overall awareness and risk mitigation among varying demographic groups [29].

Secondly, organizations and individuals must prioritize the enhancement of cybersecurity knowledge. This can be achieved through continuous training initiatives, awareness campaigns, and the dissemination of educational resources that equip users with the requisite skills to identify and effectively manage cybersecurity risks.

Thirdly, the study highlights the importance of addressing psychological factors, such as optimism bias, to promote cybersecurity awareness and behaviour. Strategies should be formulated to challenge cognitive biases and encourage a more realistic assessment of cybersecurity risks.

Furthermore, the study suggests that support systems should be established to promote secure online practices, helping individuals transition from their current habits to more effective cybersecurity practices [30]. This may involve the application of incentives, social norms, or other behavioural interventions to persuade users to adopt secure habits.

5. CONCLUSION

Cybersecurity awareness constitutes a multifaceted issue influenced by numerous factors, including demographics, knowledge, psychological biases, and contextual elements. The findings of this study underscore the necessity for comprehensive strategies that take into consideration these factors to advance cybersecurity awareness and responsible online behaviour. These results enhance our comprehension of the relationship between human factors and cybersecurity behaviours, and they may inform the development of training and intervention initiatives aimed at mitigating risky cybersecurity practices. Cybersecurity parallels sociotechnical systems, with an increase in the sophistication and frequency of attacks on organisations and governments [2]. To address cybersecurity challenges, institutions can implement strategies to raise awareness of cybersecurity and encourage individuals to pursue careers in the field. Game-based techniques have proven effective in fostering students' awareness of cybersecurity and stimulating their interest in related careers [31]. However, many users possess a limited understanding of the risks associated with being online and have yet to engage in cybersecurity education or training programs [32]. Individual choices and decision-making processes are outcomes that accentuate the importance of understanding these psychological factors [33]. It is crucial to design systems that render security procedures more user-friendly, as evidenced by the increasing utilisation of biometric data. Fear-based initiatives are generally less effective in the realm of cybersecurity, as the solutions and risks are perpetually evolving. To cultivate effective cybersecurity awareness and encourage safe online behaviour, it is imperative to address psychological factors, such as optimism bias, and customise programs for specific demographics [31], [34]. In addition,

Vol. 6, No. 4, August 2025, Page. 1897-1910
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4861

organisations need to emphasise continuous education, offer tailored messaging, and establish support systems to promote secure habits and reduce cybersecurity risks [35], [36], [37]. Cybersecurity demands a diverse array of skills, encompassing non-technical abilities such as communication, critical thinking, problem-solving, and technical expertise [38]. The qualities above are vital for cybersecurity professionals to comprehend complex risks, make informed decisions, and effectively articulate security measures to various stakeholders [39]. The establishment of digital platforms and online learning environments has resulted in increased funding for cybersecurity courses and accompanying awareness initiatives in higher education institutions [40]. Cybersecurity education must strike a delicate balance between theoretical knowledge and practical applications to adequately prepare security professionals. Furthermore, providing interdisciplinary courses can facilitate students from diverse academic backgrounds in grasping the fundamentals of cybersecurity. To maintain competitiveness in the rapidly evolving cybersecurity landscape, cybersecurity curricula must adapt to include the latest trends and risks [40].

In summary, enhancing cybersecurity awareness among information systems users necessitates a thorough approach that considers demographic factors, knowledge levels, psychological biases, and the broader environment. By tailoring awareness initiatives to specific audiences, prioritising cybersecurity knowledge, addressing psychological biases, and instituting support systems for behavioural modification, organisations can cultivate more resilient and secure digital ecosystems [41]. Cybersecurity education must be continually updated to keep pace with the rapidly evolving threat landscape. Cybersecurity awareness is crucial for all users because everyone is responsible for protecting it. Individuals' attitudes and behaviours regarding cybersecurity are greatly influenced by their degree of awareness. The results indicate that CA plays a crucial role in mediating the influence of antecedent factors on UBASM. Although other exogenous variables have a moderate to minor impact, this emphasises the need for strategic interventions to enhance user awareness of digital security and improve security behaviour online environment. Effective cybersecurity education and training can enhance individuals' understanding of online risks, enabling them to make informed decisions and protect themselves from cyberattacks. Educational initiatives should be implemented at all levels, from elementary schools to workplaces, to foster a culture of cybersecurity awareness. These initiatives should focus on teaching fundamental cybersecurity concepts, including phishing recognition, password security, data privacy, and safe internet browsing practices. Interactive learning techniques, such as simulations, gamification, and real-world case studies, should be incorporated into cybersecurity education programs to enhance engagement and improve knowledge retention.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest either among themselves or with the subject of this research

ACKNOWLEDGEMENT

The authors express their sincere gratitude to all parties who have provided valuable support and contributions, enabling the successful completion of this journal.

REFERENCES

[1] F. Djatsa, “Threat Perceptions, Avoidance Motivation and Security Behaviors Correlations,” *Journal of Information Security*, vol. 11, no. 1, pp. 19–45, Jun. 2019, doi: 10.4236/jis.2020.111002.

[2] C. Macabante, S. Wei, and D. Schuster, “Elements of Cyber-Cognitive Situation Awareness in Organizations,” *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 63, no. 1, pp. 1624–1628, Jun. 2019, doi: 10.1177/1071181319631483.

[3] S. Kalhoro, M. Rehman, V. Ponnusamy, and F. B. Shaikh, "Extracting Key Factors of Cyber Hygiene Behaviour Among Software Engineers: A Systematic Literature Review," *IEEE Access*, vol. 9, pp. 99339–99363, Jun. 2021, doi: 10.1109/access.2021.3097144.

[4] M. A. Helmiawan, E. Firmansyah, I. Fadil, Y. Sofivan, F. Mahardika, and A. Guntara, "Analysis of web security using open web application security project 10," *2020 8th International Conference on Cyber and IT Service Management (CITSM …*, 2020.

[5] I. Lee, "Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management," *Future Internet*, vol. 12, no. 9, p. 157, Jun. 2020, doi: 10.3390/fi12090157.

[6] C. Aksoy, "BUILDING A CYBER SECURITY CULTURE FOR RESILIENT ORGANIZATIONS AGAINST CYBER ATTACKS," *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*, vol. 7, no. 1, pp. 96–110, Jun. 2024, doi: 10.33416/baybem.1374001.

[7] S. N. S. Nasir, "Exploring the Effectiveness of Cybersecurity Training Programs: Factors, Best Practices, and Future Directions," *Advances in Multidisciplinary & Scientific Research Journal Publication*, vol. 2, no. 1, pp. 151–160, Jun. 2023, doi: 10.22624/aims/csean-smart2023p18.

[8] B. Uchendu, J. R. C. Nurse, M. Bada, and S. Furnell, "Developing a cyber security culture: Current practices and future needs," *Comput Secur*, vol. 109, p. 102387, Jun. 2021, doi: 10.1016/j.cose.2021.102387.

[9] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework," *Sensors*, vol. 21, no. 9, p. 3267, Jun. 2021, doi: 10.3390/s21093267.

[10] W. A. Cram, J. G. Proudfoot, and J. D'Arcy, "Organizational information security policies: a review and research framework," Jun. 2017, *Palgrave Macmillan*. doi: 10.1057/s41303-017-0059-9.

[11] G. Özaslan *et al.*, "EVALUATION OF THE EFFECTS OF INFORMATION SECURITY TRAINING ON EMPLOYEES: A STUDY FROM A PRIVATE HOSPITAL," *International Journal of Health Management and Tourism*, Jun. 2020, doi: 10.31201/ijhmt.791913.

[12] A. Sopandi, N. A. Yahaya, and A. Subiyakto, "Developing the Readiness and Success Model of Information System Implementation in the Indonesian Equestrian Industry," *Journal of Applied Data Sciences*, vol. 5, no. 1, pp. 133–145, 2024.

[13] A. D. K. Acquaye, "A Study of the Awareness of Security and Safety Culture Among Employees Across Organizations," *Texila international journal of management*, pp. 115–128, Jun. 2020, doi: 10.21522/tijmg.2015.se.19.02.art013.

[14] A. Tolah, S. Furnell, and M. Papadaki, "A Comprehensive Framework for Understanding Security Culture in Organizations," in *IFIP advances in information and communication technology*, Springer Science+Business Media, 2019, pp. 143–156. doi: 10.1007/978-3-030-23451-5_11.

[15] M. A. Helmiawan, I. Fadil, Y. Sofiyan, and E. Firmansyah, "Security model using intrusion detection system on cloud computing security management," *2021 9th International Conference on Cyber and IT Service Management (CITSM …*, 2021.

[16] A. P. Diman and T. K. A. Rahman, "Examining individual tendency to respond to phishing e-mails from the perspective of protection motivation theory," *Journal of Education and Social Sciences*, vol. 25, no. 1, pp. 40–51, 2023.

[17] I. Musirin, S. I. Sulaiman, T. K. A. Rahman, S. Shaari, A. M. Omar, and ..., "Computational performance of artificial immune system-based sizing technique for grid-connected photovoltaic system," *Research Management Institute (RMI)*, 2012.

[18] M. S. Hasan, R. A. Rahman, S. F. H. B. T. Abdillah, and N. Omar, "Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia," *Journal of Social Sciences*, vol. 11, no. 4, pp. 395–404, Jun. 2015, doi: 10.3844/jssp.2015.395.404.

[19] T. Alharbi and A. Tassaddiq, "Assessment of Cybersecurity Awareness among Students of Majmaah University," *Big Data and Cognitive Computing*, vol. 5, no. 2, p. 23, Jun. 2021, doi: 10.3390/bdcc5020023.

[20] C. G. Blackwood-Brown, Y. Levy, and J. D'Arcy, "Cybersecurity Awareness and Skills of Senior Citizens: A Motivation Perspective," *Journal of Computer Information Systems*, vol. 61, no. 3, pp. 195–206, Jun. 2019, doi: 10.1080/08874417.2019.1579076.

Vol. 6, No. 4, August 2025, Page. 1897-1910
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4861

[21] V. Karagiannopoulos, A. Kirby, S. Oftadeh-Moghadam, and L. Sugiura, "Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study," *Computer Law & Security Review*, vol. 43, p. 105615, Jun. 2021, doi: 10.1016/j.clsr.2021.105615.

[22] P. van Schaik, K. Renaud, C. Wilson, J. Jansen, and J. Onibokun, "Risk as affect: The affect heuristic in cybersecurity," *Comput Secur*, vol. 90, p. 101651, Jun. 2019, doi: 10.1016/j.cose.2019.101651.

[23] A. R. Neigel, V. L. Claypoole, G. E. Waldfogle, S. Acharya, and G. M. Hancock, "Holistic cyber hygiene education: Accounting for the human factors," *Comput Secur*, vol. 92, p. 101731, Jun. 2020, doi: 10.1016/j.cose.2020.101731.

[24] F. L. Greitzer, W. Li, K. B. Laskey, J. Lee, and J. Purl, "Experimental Investigation of Technical and Human Factors Related to Phishing Susceptibility," *ACM Transactions on Social Computing*, vol. 4, no. 2, pp. 1–48, Jun. 2021, doi: 10.1145/3461672.

[25] Y. Chen, I. YeckehZaare, and A. F. Zhang, "Real or bogus: Predicting susceptibility to phishing with economic experiments," *PLoS One*, vol. 13, no. 6, Jun. 2018, doi: 10.1371/journal.pone.0198213.

[26] N. Beu *et al.*, "Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation," *Comput Secur*, vol. 131, p. 103313, Jun. 2023, doi: 10.1016/j.cose.2023.103313.

[27] H. J. Parker and S. Flowerday, "Contributing factors to increased susceptibility to social media phishing attacks," *S Afr J Inf Manag*, vol. 22, no. 1, Jun. 2020, doi: 10.4102/sajim.v22i1.1176.

[28] T. Lin *et al.*, "Susceptibility to Spear-Phishing Emails," *ACM Transactions on Computer-Human Interaction*, vol. 26, no. 5, pp. 1–28, Jun. 2019, doi: 10.1145/3336141.

[29] W. J. Triplett, "Addressing Cybersecurity Challenges in Education," *International Journal of STEM Education for Sustainability*, vol. 3, no. 1, pp. 47–67, Jun. 2023, doi: 10.53889/ijses.v3i1.132.

[30] R. Shillair, P. Esteve-González, W. H. Dutton, S. Creese, E. Nagyfejeo, and B. von Solms, "Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise," *Comput Secur*, vol. 119, p. 102756, Jun. 2022, doi: 10.1016/j.cose.2022.102756.

[31] W. Aljohni, N. Elfadil, M. A. Jarajreh, and M. Gasmelsied, "Cybersecurity Awareness Level: The Case of Saudi Arabia University Students," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 3, Jun. 2021, doi: 10.14569/ijacsa.2021.0120334.

[32] A. Alzahrani, "Assessing and Proposing Countermeasures for Cyber-Security Attacks," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 1, Jun. 2022, doi: 10.14569/ijacsa.2022.01301102.

[33] H. Taherdoost, "Towards an Innovative Model for Cybersecurity Awareness Training," *Information*, vol. 15, no. 9, p. 512, Jun. 2024, doi: 10.3390/info15090512.

[34] E. Stavrou and andriani Piki, "Cultivating self-efficacy to empower professionals' re-up skilling in cybersecurity," *Information and Computer Security*, vol. 32, no. 4, pp. 523–541, Jun. 2024, doi: 10.1108/ics-02-2024-0038.

[35] L. S. Setianingsih, R. Pulungan, A. E. Putra, M. E. Wibowo, and S. Syarip, "Risk Assessment Methods for Cybersecurity in Nuclear Facilities: Compliance to Regulatory Requirements," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 9, Jun. 2021, doi: 10.14569/ijacsa.2021.0120979.

[36] M. Mukherjee, N. T. Le, Y.-W. Chow, and W. Susilo, "Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes," *Information*, vol. 15, no. 2, p. 117, Jun. 2024, doi: 10.3390/info15020117.

[37] D. Patole, P. Ahirao, and Y. Borse, "Novel Teaching Learning and Evaluation Activities for Imbibing the Concepts of Cyber Security as Perennial Thought-Process in the Learners' Digital Life," *Journal of Engineering Education/Journal of engineering education transformations/Journal of engineering education transformation*, vol. 33, p. 376, Jun. 2020, doi: 10.16920/jeet/2020/v33i0/150204.

Vol. 6, No. 4, August 2025, Page. 1897-1910
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4861

[38] J. Hajný, S. Ricci, E. Piesarskas, O. Levillain, L. Galletta, and R. De Nicola, "Framework, Tools and Good Practices for Cybersecurity Curricula," *IEEE Access*, vol. 9, pp. 94723–94747, Jun. 2021, doi: 10.1109/access.2021.3093952.

[39] J. Dawson and R. Thomson, "The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance," Jun. 2018, *Frontiers Media*. doi: 10.3389/fpsyg.2018.00744.

[40] V. Švábenský, J. Vykopal, M. Čermák, and M. Laštovička, "Enhancing cybersecurity skills by creating serious games," Jun. 2018, doi: 10.1145/3197091.3197123.

[41] S. M. Redman, K. J. Yaxley, and K. Joiner, "Improving General Undergraduate Cyber Security Education: A Responsibility for All Universities?," *Creat Educ*, vol. 11, no. 12, pp. 2541–2558, Jun. 2020, doi: 10.4236/ce.2020.1112187.