Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4, 2954-2963
2025
Publisher: Learning Gate
DOI: 10.55214/25768484.v9i4.6701

The role of accounting employees' information security awareness on the intention to resist social engineering

Rian Candy Senduk[1*], Yohannes Kurniawan[2]
[1]Accounting Department, School of Accounting, Master of Accounting, Bina Nusantara University, Jakarta, Indonesia, 11480; rian.senduk@binus.ac.id (R.C.S.).
[2]Information Systems Department, School of Information systems, Bina Nusantara University, Jakarta, Indonesia, 11480; ykurniawan@binus.edu (Y.K.).

Abstract: The growing reliance on technology in accounting has boosted productivity but also increased vulnerability to cyber threats, particularly social engineering attacks that exploit human weaknesses to access sensitive data. This study evaluates and enhances security awareness among accounting employees to mitigate risks for individuals and organizations. Using a questionnaire survey and SmartPLS 4.1.0.9, it tests 12 hypotheses derived from prior research, assessing the Theory of Planned Behavior's applicability in explaining employees' resistance to social engineering. The study focuses on accountants in medium-to-large firms in Indonesia's Jabodetabek region, including senior managers, first-level managers, and entry-level employees, with an emphasis on recent five-year data breaches. Results show high overall security awareness, but six hypotheses were insignificant, indicating that TPB does not fully explain employees' intentions to counter such threats. While findings underscore strong awareness, the partial support for TPB highlights the need for further research on behavioral influences. The study stresses the importance of organizational and individual vigilance in safeguarding credentials, urging accountants to adopt proactive measures against social engineering. It also lays the groundwork for future research on improving cybersecurity performance in accounting. Given limited prior studies on accounting-specific security awareness, this work offers key insights for practitioners and academics.

Keywords: *Cyberthreats, Information security awareness, Social engineering, Theory of planned behavior.*

1. Introduction

Digital transformation is not only limited to the technology business; this process covers firms of all sizes and industry diversity [1]. Accountants are responsible for sustainable resource management and company, individual, and environmental development, which limits their technological use [2]. Accounting systems that need to identify, integrate, process, calculate, categorize, record and report can be completed quickly due to technological developments to help make final decisions and increase transparency [3]. Application of technology in accounting brings benefits such as reduced costs, security, convenience, and increased integration and reconciliation in real time [4]. It has been proven that the use of technology in accounting work has increased the world economy by 575 million USD according to IFAC (International Federation of Accountants) 2015. However, accountants' dependence on modern and automated technology certainly raises concerns about future risks. Andiola et al states that the integration of technology in accounting doesn't guarantee effective understanding or proficient use [5]. Technology in accounting poses risks like financial data leaks, requiring greater focus on risk assessment [6]. This also needs to be considered to maintain the reputation and credibility of a company Safa et al stated that the development of information security technology needs to be considered not only from a technological aspect but also from a human aspect [7]. In reality, a

History: Received: 28 February 2025; Revised: 14 April 2025; Accepted: 17 April 2025; Published: 29 April 2025
* Correspondence: rian.senduk@binus.ac.id

significant majority of organizational information security problems are produced by the exploitation of the human element [8]. According to ENISA (The European Union Agency for Cybersecurity) 2019, 77% of companies' data leaks exploit human weaknesses. Credential information leaks via phishing (e-mail) are financially impacted with an average of 4.88 million USD per company in 2024 and it takes over 100 days for companies to recover from the incident according to IBM (International Business Machine Co.) 2024. Information security is crucial for accountants, making many companies compete to improve their security systems, even spending a lot of money [9] according to IDC (International Data Corporation) 2024 companies spent 119.9 billion USD to improve information security in 2021. Accounting employees, as key assets, must be prioritized in protecting personal and company information [10].

Information security knowledge reflects a company's readiness to prevent cyber-attacks like social engineering [11]. Boosting information security awareness involves not only technical systems but also nontechnical [12]. The influence of management or leadership can increase information security awareness to determine rules and become a role model for subordinates [13] as well as assessments of attitudes, behavior, culture, and work habits of employees in the company [8] other factors are followed by information security policies, education and training [14].

Cybersecurity incidents cause financial and reputational harm, with social engineering posing a major threat due to human involvement in technology access [15]. Social engineering threatens system security by manipulating victims to leak credentials or follow commands, as humans are the weakest link in a company's security chain [16]. A 2024 Verizon survey found that credential leaks from social engineering were primarily caused by pretexting, phishing, and web applications, exposing 3,661 pieces of personal data, with most leaks occurring in large-scale companies in Indonesia, data leaks at e-commerce companies exposed 91 million user records and 21,000 identity-related data, highlighting the need to improve information security and accounting employees' awareness to combat cyber-attacks like social engineering. This study focuses on accountants in the Jabodetabek area, as they are considered a source of cyber-attacks according to Indonesia's Ministry of Communication and Digital Affairs' Digital Society Index. This research is limited to medium and large companies because they generally have a clearer management structure, financial and security systems. This study aims to fill research gaps and highlight the importance of information security awareness for companies and accounting employees.

2. Literature Review, Research Framework and Hypothesis

Increasing information security awareness to prevent social engineering relies not only on the organization but also on individual behavior, assessed using the TPB (Theory of Planned Behavior to predict behavioral intentions [17]. TPB, a development of the Theory of Reasoned Action (TRA), explains individual decision-making processes for adoption by companies [18]. Understanding these issues provides valuable insights to help organizations and accounting employees boost information security awareness and advance knowledge in this field [19]. The development of technology indicates that more and more weaknesses or gaps in a technology are experiencing cyber attacks and human factors will not be separated from technology, no matter how sophisticated the technology is [20]. The human factor is the weakest link in a company's security chain, exploited by perpetrators to obtain the desired information or assets because it is easier than trying to break into a sophisticated technological system [21]. This study examines factors influencing information security awareness and behavioral attitudes of accounting employees based on the TPB theory, which predicts intentions to resist social engineering. These factors include Leadership, Trust, Risk, Information Security Policies, SETA program, Awareness, Attitude, Perceived Behavioral Control, Subjective Norms, and Intention (Figure 1).

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 2954-2963, 2025
DOI: 10.55214/25768484.v9i4.6701

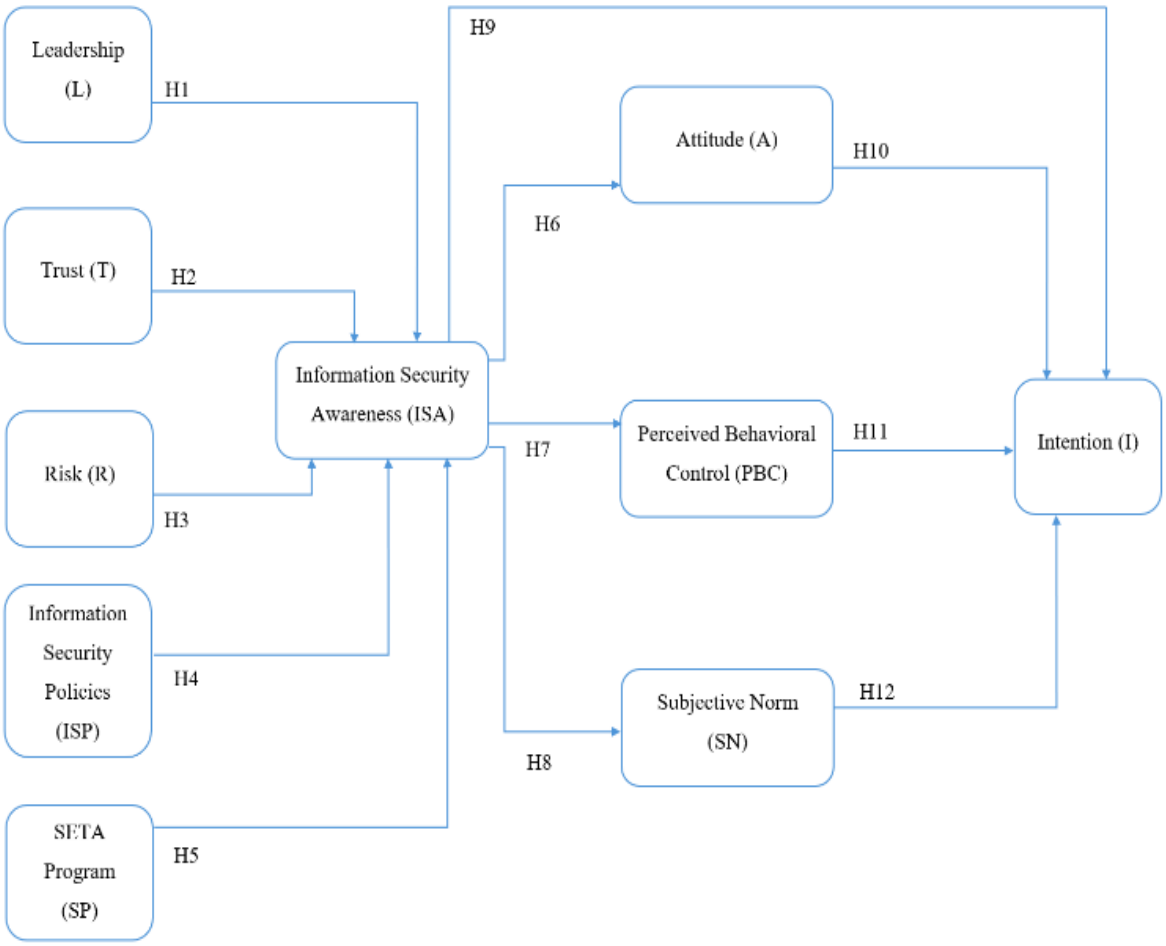

Figure 1.
Theoretical Framework.

2.1. Hypothesis

H1: Leadership (L) has a positive impact on the information security awareness (ISA) of accounting employees.

H2: The tendency of Trust (T) has a positive impact on accounting employees' ISA.

H3: The tendency to take Risks (R) positively affects the ISA of accounting employees.

H4: Information Security Policies (ISP) have a positive impact on the ISA of accounting employees.

H5: SETA Programs (SP) have a positive impact on the ISA of accounting employees.

H6: Accounting employees' ISA has a positive impact on Attitudes (A)

H7: Accounting employees' ISA has a positive impact on Perceived Behavioral Control (PBC)

H8: Accounting employees' ISA has a positive impact on Subjective Norm (SN).

H9: Accounting employees' ISA has a positive impact on their Intention (I) to resist social engineering.

H10: The attitude of accounting employees positively affects their intention to resist social engineering attacks.

H11: The perceived behavioral control of accounting employees positively affects their intention to resist social engineering attacks.

H12: The accounting employees' subjective norm positively affects their intention to resist social engineering attacks.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 2954-2963, 2025
DOI: 10.55214/25768484.v9i4.6701

3. Methods

This research uses quantitative methods to test hypotheses empirically, focusing on accounting employees below c-level in large and medium-scale companies in the Jabodetabek area of Indonesia. Data collection was carried out by distributing questionnaires via google form and other social media starting from November 12, 2024, to December 12, 2024. The research variables are presented in the form of a questionnaire to respondents using a 4-point Likert scale starting from strongly disagree (1) to strongly agree (4). This scale is used to avoid neutral answers and to make the response direction clearer. The population in this study is only known from the information of the Ministry of Manpower of the Republic of Indonesia, the number of medium to large-scale companies up to 66,446 companies in total, where the number of accounting employees with positions below c-level in medium to large-scale companies in the Jabodetabek area of Indonesia is unknown. Therefore, the sampling technique in this study adopted research from Roscoe which was developed in 1975 [22]. Then the calculation of the research sample has a minimum of 30 respondents to avoid error calculations in the SmartPLS ver 4.1.0.9 application [23]. Data analysis in this study used SEM (Structure Equation Modeling) with the PLS (Partial Least Square) approach, because it can measure variance and handle latent variables and is suitable for measuring components of the TPB [17]. In the last one to two decades, SEM-PLS has been used more in discussing strategic and operational accounting in companies. SEM-PLS in the application of research with a tendency to be complex to the variable indicators, constructs and many structures can help researchers predict information related to the relationship between variables [24]. The initial procedure in SEM-PLS is to determine the validity and reliability of each indicator. The validity tests include convergent validity, average variance extracted, and discriminant validity [23]. The reliability test uses Cronbach's alpha and composite reliability, followed by the hypothesis test implementing the bootstrapping test [24]. The data from this research can be accessed through our open data portal [http://bit.ly/4cJF4aC]. By making this research data publicly available, we aim to support further study and encourage collaboration across various fields.

4. Results and Discussion

The data successfully collected amounted to 200 respondents with profiles that match those in Table 1. Based on gender, it is dominated by male at 52%, in terms of age it is dominated by the 25-34 year group, the company scale based on employees is dominated by the medium scale, and the accommodation industry is the highest, while for work experience, it is dominated by the 1-5 year group, then for job positions the most are first level managers followed by entry level which are found in Table 1.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 2954-2963, 2025
DOI: 10.55214/25768484.v9i4.6701

Table 1.
Demographic Data of the Respondents.

Category	Description	Frequency	Percentage
Company Scale	20-100 (middle)	133	66.5%
	>100 (big)	67	33.5%
Industry	Accomodation	34	17.0%
	Finance	32	16.0%
	Administration	28	14.0%
	Manufacture	20	10.0%
	Construction	17	8.5%
	Technology	16	8.0%
	Property & Transportation	16	8%
	Retail	14	7.0%
	Health	7	3.5%
	Others	16	8%
Working Experience	< 1 year	29	14.5%
	1-5 years	119	59.5%
	> 5 years	52	26.0%
Job Position	Senior Manager	51	25.5%
	First Level Manager	75	37.5%
	Entry Level	74	37.0%

The obtained questionnaire data is then processed using the SmartPLS ver 4.1.0.9 application to calculate and analyze the research results. The application's objective is to support this research, which employs the SEM-PLS approach, beginning with convergent validity, discriminant validity, the Fornell-Larcker test, and hypothesis testing. The following figure shows a structural model of the study.

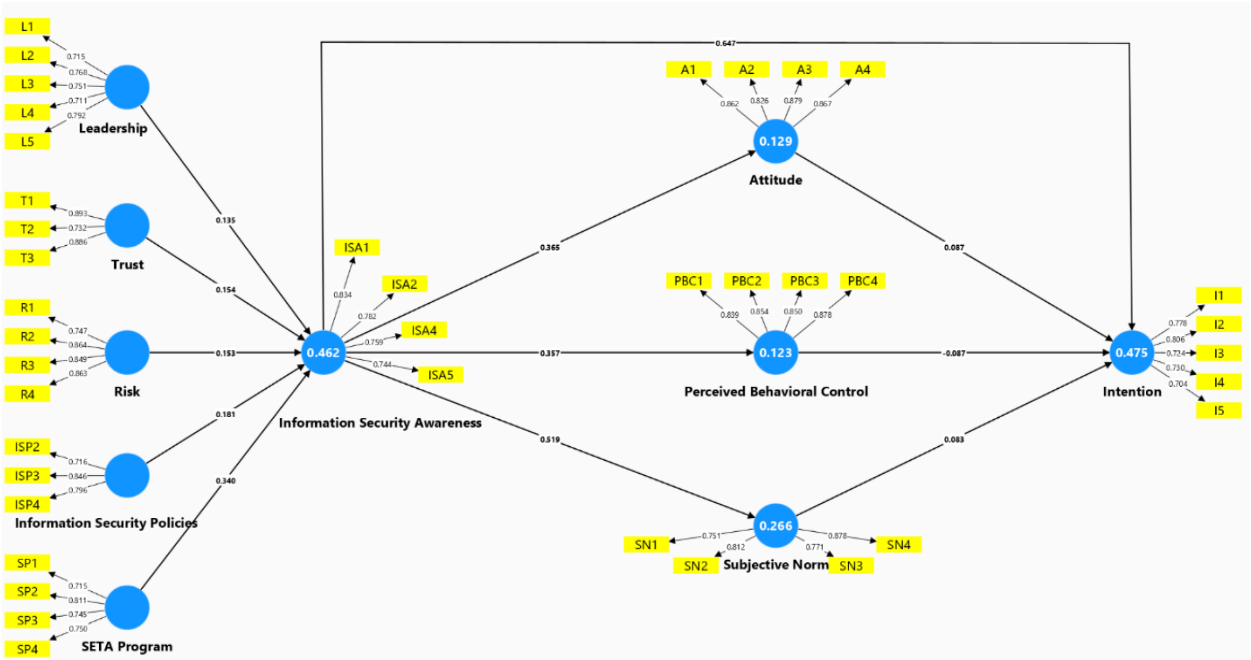

Figure 2.
Structural Model.

As shown in Figure 2, the structural model excludes the ISP1 and ISP5 indicators and the ISA3 indicator due to loading factors below 0.70. According to Hair and Alamer, indicators should exceed 0.70 to ensure high data validity and improve the relevance and accuracy of the analysis [24].

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 2954-2963, 2025
DOI: 10.55214/25768484.v9i4.6701

4.1. Validity Analysis

According to Hair and Alamer, validity testing is essential to ensure accurate and reliable data for subsequent analysis [24]. Convergent validity assesses data readability and research indicators, while Table 2 displays the links among the study model's latent variables.

Table 2.
Convergent Validity Test.

Construct	Item	Outer Loadings	Indicator
Leadership (L)	L1	0.715	The appropriate level of knowledge and skills in information security
	L2	0.768	Leaders promote understanding, cooperation, and communication
	L3	0.751	Leaders firmly give rewards for disobeying information security rules
	L4	0.711	Company leaders describe information security as a collective effort
	L5	0.792	leaders describe information security as a function that supports business
Trust (T)	T1	0.893	Trust people until the trusted person gives me a reason
	T2	0.732	Trust people but have doubts when we first meet them
	T3	0.886	Trust new acquaintances
Risk (R)	R1	0.747	Providing information to other parties would be risky
	R2	0.864	There will be a high potential for loss
	R3	0.849	There will be a lot of uncertainty
	R4	0.863	Providing information to another party
Information Security Policies (ISP)	ISP2	0.716	Complying with the company's information security policy
	ISP3	0.846	Careful compliance with information security policies
	ISP4	0.796	The information security policies will reduce the likelihood of information
SETA Program (SP)	SP1	0.715	Procedures regarding company information security training
	SP2	0.811	Optimizing the method, level of information, and media of Company
	SP3	0.745	Training and education runs regularly to help employees *up to date*
	SP4	0.750	The Security Education Training Awareness (SETA) Program motivated
Information Security Awareness (ISA)	ISA1	0.834	Aware that if I do not adopt appropriate information security behavior
	ISA2	0.782	Aware that it is a serious problem if organizational data is stolen
	ISA4	0.759	Information security precautions are effective for protecting
	ISA5	0.744	I understand the risks posed by inadequate information security in general
Attitude (A)	A1	0.862	A positive attitude or response to identify unexpected and unauthorized
	A2	0.826	A positive attitude or response to discourage individuals
	A3	0.879	A positive attitude or response suspicious requests in email
	A4	0.867	A positive attitude towards preventing unauthorized individuals
Perceived Behavioral Control (PBC)	PBC1	0.839	A behavioral controls to identify unexpected and unauthorized
	PBC2	0.854	A behavioral controls to prevent individuals from *software* dangerous
	PBC3	0.850	A positive behavioral controls to suspicious requests in email

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 2954-2963, 2025
DOI: 10.55214/25768484.v9i4.6701

	PBC4	0.878	A behavioral controls to prevent accessing confidential information
Subjective Norm (SN)	SN1	0.751	People around me think that I will identify unexpected and unauthorized,
	SN2	0.812	People around me think that I will prevent other people
	SN3	0.771	People around me think that I will identify suspicious requests in emails
	SN4	0.878	People around me think that I will prevent unauthorized individuals
Intention (I)	I1	0.778	Suspect is not a legitimate party or authority to receive such information
	I2	0.806	Prevent gaining access to my work devices for reasons of security attacks
	I3	0.724	Install *software* if I suspect the request came from an unauthorized sender
	I4	0.730	Suspect of being an unauthorized person
	I5	0.704	intention of disclosing *password* my work device to anyone

Discriminant validity is determined by evaluating cross-loading, where an indicator's loading value for its variable must exceed those for other variables [3]. Outer loadings testing revealed that ISP1, ISP5, and ISA3 indicators fell below the validity threshold of >0.70 for convergent validity and were therefore eliminated. To ensure construct validity and qualified discriminant values, Fornell-Larcker testing was applied. The results, confirming the data meets discriminant validity criteria, are available at: https://bit.ly/3VBUDtF.

4.2. Reliability Test

Reliability testing assesses the consistency and trustworthiness of a measurement tool. It follows validity testing, as unreliable data cannot be valid. Construct reliability is evaluated using Composite Reliability (CR) and Cronbach's Alpha (CA), both requiring values >0.7 for reliability, while Average Variance Extracted (AVE) must exceed 0.50 [25].

Table 3.
Construct Validity, Reliability Data, and R-Square Test.

Variable	CA	rho_a	CR	AVE	R-Square	R-Square Adjusted
L	0.804	0.815	0.864	0.559		
T	0.792	0.829	0.877	0.706		
R	0.852	0.870	0.900	0.692		
ISP	0.702	0.743	0.830	0.620		
SP	0.751	0.760	0.842	0.572		
ISA	0.785	0.791	0.861	0.609	0.475	0.462
A	0.881	0.881	0.918	0.738	0.133	0.129
PBC	0.879	0.891	0.916	0.732	0.128	0.123
SN	0.824	0.874	0.880	0.647	0.269	0.266
I	0.805	0.810	0.865	0.562	0.485	0.475

The determinant coefficient measures the influence of independent variables on a dependent variable. It classifies impact levels as weak (0.19), moderate (0.33), or strong (0.67). A value closer to 1 indicates the independent variable provides nearly all the information needed to predict the dependent variable [24]. Data from SmartPLS ver 4.1.0.9 in Table 3 shows that intermediary variables—information security awareness, attitude, perceived behavioral control, and subjective norm—explain 48.5% of the intention variable. This places the intention variable between moderate and strong classifications.

4.3. Hypothesis Testing

After completing validity and reliability tests, hypothesis testing was conducted using bootstrapping in SmartPLS ver 4.1.0.9. If the p-value <0.05 or t-statistic >1.96, the results are considered significant, and the indicator is valid for measuring latent variables [26]. The hypothesis testing results for each latent variable are shown in Table 4.

Table 4.
Hypothesis Testing (Bootstrapping).

Construct	T-statistic	P-Values
Leadership --> Information Security Awareness	1.702	0.089
Trust --> Information Security Awareness	2.229	0.026
Risk --> Information Security Awareness	1.849	0.065
Information Security Policies --> Information Security Awareness	1.753	0.080
SETA Program --> Information Security Awareness	3.532	0.000
Information Security Awareness --> Attitude	4.901	0.000
Information Security Awareness --> Perceived Behavioral Control	4.719	0.000
Information Security Awareness --> Subjective Norm	9.670	0.000
Information Security Awareness --> Intention	9.631	0.000
Attitude --> Intention	0.837	0.402
Perceived Behavioral Control --> Intention	0.824	0.410
Subjective Norm --> Intention	1.049	0.294

Hypothesis testing is a statistical method used to determine if sample data supports or rejects a hypothesis about a population [27]. It is a decision-making process that evaluates if observed data supports or contradicts the assumed hypothesis. Hypothesis testing is a scientific method used to evaluate hypotheses by comparing observed data to expectations, determining if the evidence supports or refutes the initial claim. It is crucial in scientific research and decision-making. Table 4 reveals the hypothesis testing results, showing H1, H3, H4, H10, H11, and H12 with t-statistic values below the threshold and p-values above the normal range. In contrast, H2, H5, H6, H7, H8, and H9 have t-statistic values >1.96 and p-values <0.05, indicating significant relationships. More details the hypothesis measurements reveal varying levels of significance based on P-values and T-statistics. H1 has a P-value of 0.089 and a T-statistic of 1.702, indicating insignificance. H2 is significant with a P-value of 0.026 and a T-statistic of 2.229. H3 and H4 are insignificant, with P-values of 0.065 and 0.080 and T-statistics of 1.849 and 1.753, respectively. H5 shows significance with a P-value of 0.000 and a T-statistic of 3.532. Similarly, H6, H7, H8, and H9 are significant, all having P-values of 0.000 and T-statistics of 4.901, 4.901, 9.670, and 9.631. Conversely, H10, H11, and H12 are insignificant, with P-values of 0.402, 0.410, and 0.294 and T-statistics of 0.837, 0.824, and 1.049. This study's findings reveal several key points: H1 shows leadership has a positive but insignificant impact on accounting employees' security awareness, aligning with previous research. H2 indicates trust significantly affects awareness, consistent with studies highlighting trust's negative impact. H3 finds risk has a positive but insignificant relationship with awareness. H4 shows security policies have a positive but insignificant impact. H5 confirms SETA programs significantly affect awareness. H6, H7, and H8 demonstrate that information security awareness significantly influences attitudes, perceived behavioral control, and subjective norms. H9 reveals that awareness significantly impacts the intention to resist social engineering, while H10, H11, and H12 show that attitudes, perceived behavioral control, and subjective norms have a positive but insignificant effect on this intention.

5. Conclusion

This study aims to enhance security awareness among accounting employees in protecting credential information, reducing risks for individuals and organizations. Based on 12 hypotheses developed from previous research, the results show positive impacts, though 6 hypotheses (H1, H3, H4, H10, H11, H12) were insignificant according to SmartPLS ver 4.1.0.9 testing, suggesting TPB theory

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 2954-2963, 2025
DOI: 10.55214/25768484.v9i4.6701

doesn't fully support accounting employees' intention to resist social engineering. A questionnaire survey reveals high information security awareness among individuals and organizations. The research is limited to accountants in medium to large-scale companies in the Jabodetabek area of Indonesia, focusing on data breaches reported in the last five years, and includes senior, first-level managers, and entry-level employees. Due to limited prior research on accounting information security awareness, this study emphasizes both organizational and individual awareness based on TPB theory. It encourages accountants to protect credentials and avoid cyber-attacks, particularly social engineering, and provides a foundation for further research on improving organizational performance in safeguarding credential information.

Institutional Review Board Statement:

Informed Consent: All participants provided written informed consent before participating in the study. They were informed of the research purpose, procedures, potential risks, and their right to withdraw at any time without penalty. Confidentiality: Participant data were anonymized and stored securely, with access restricted to the research team. No personally identifiable information was disclosed in the study's findings. Compliance: The research adhered to the ethical principles outlined in the APA Ethical Guidelines and relevant institutional policies.

Transparency:

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

Acknowledgement:

Author contributions: Conceptualization, YK (Yohannes Kurniawan); methodology, YK and RCS (Rian Candy Senduk); software, RCS; validation, RCS; formal analysis, RCS; investigation, YK and RCS; resources, RCS (Rian Candy Senduk); data curation, YK; writing—original draft preparation, RCS; writing—review and editing, YK; visualization, RCS; supervision, YK; project administration, YK; funding acquisition, RCS. All authors have read and agreed to the published version of the manuscript.

References

[1] K. S. Warner and M. Wäger, "Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal," *Long Range Planning*, vol. 52, no. 3, pp. 326-349, 2019. https://doi.org/10.1016/j.lrp.2018.12.001

[2] G. Carnegie, L. Parker, and E. Tsahuridu, "It's 2020: What is accounting today?," *Australian Accounting Review*, vol. 31, no. 1, pp. 65-73, 2021. https://doi.org/10.1111/auar.12325

[3] S. Yoon, "A study on the transformation of accounting based on new technologies: Evidence from Korea," *Sustainability*, vol. 12, no. 20, p. 8669, 2020. https://doi.org/10.3390/su12208669

[4] K. Phornlaphatrachakorn and K. Na Kalasindhu, "Digital accounting, financial reporting quality and digital transformation: Evidence from Thai listed firms," *The Journal of Asian Finance, Economics and Business*, vol. 8, no. 8, pp. 409-419, 2021. https://doi.org/10.13106/jafeb.2021.vol8.no8.0409

[5] L. M. Andiola, E. Masters, and C. Norman, "Integrating technology and data analytic skills into the accounting curriculum: Accounting department leaders' experiences and insights," *Journal of Accounting Education*, vol. 50, p. 100655, 2020. https://doi.org/10.1016/j.jaccedu.2020.100655

[6] Q. A. Al-Fatlawi, D. S. Al Farttoosi, and A. H. Almagtome, "Accounting information security and it governance under cobit 5 framework: A case study," *Webology*, vol. 18, no. 02, pp. 294-310, 2021. https://doi.org/10.14704/web/v18si02/web18073

[7] N. S. Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," *Computers & security*, vol. 56, pp. 70-82, 2016. https://doi.org/10.1016/j.cose.2015.10.006

[8] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," *Computers & Security*, vol. 106, p. 102267, 2021. https://doi.org/10.1016/j.cose.2021.102267

[9] H. Li, S. Yoo, and W. J. Kettinger, "The roles of IT strategies and security investments in reducing organizational security breaches," *Journal of Management Information Systems*, vol. 38, no. 1, pp. 222-245, 2021. https://doi.org/10.1080/07421222.2021.1870390

[10] Y. Yang and Z. Yin, "Accountancy for E-Business Enterprises based on cyber security," *International Journal of Data Warehousing and Mining*, vol. 19, no. 6, pp. 1-17, 2023. https://doi.org/10.4018/ijdwm.320227

[11] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: A comparative study," *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 82-97, 2022. https://doi.org/10.1080/08874417.2020.1712269

[12] A. Koohang, J. Anderson, J. H. Nord, and J. Paliszkiewicz, "Building an awareness-centered information security policy compliance model," *Industrial Management & Data Systems*, vol. 120, no. 1, pp. 231-247, 2020. https://doi.org/10.1108/imds-07-2019-0412

[13] N. Guhr, B. Lebek, and M. H. Breitner, "The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory," *Information Systems Journal*, vol. 29, no. 2, pp. 340-362, 2019. https://doi.org/10.1111/isj.12202

[14] I. Al-Shanfari, W. Yassin, N. Tabook, R. Ismail, and A. Ismail, "Determinants of information security awareness and behaviour strategies in public sector organizations among employees," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 8, pp. 748–755, 2022. https://doi.org/10.14569/IJACSA.2022.0130855

[15] Z. Wang, L. Sun, and H. Zhu, "Defining social engineering in cybersecurity," *IEEe Access*, vol. 8, pp. 85094-85115, 2020. https://doi.org/10.1109/access.2020.2992807

[16] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, vol. 11, no. 4, pp. 1–20, 2019. https://doi.org/10.3390/fi11040089

[17] T. Grassegger and D. Nedbal, "The role of employees' information security awareness on the intention to resist social engineering," *Procedia Computer Science*, vol. 181, pp. 59-66, 2021. https://doi.org/10.1016/j.procs.2021.01.103

[18] Y. H. S. Al-Mamary and M. M. Alraja, "Understanding entrepreneurship intention and behavior in the light of TPB model from the digital entrepreneurship perspective," *International Journal of Information Management Data Insights*, vol. 2, no. 2, p. 100106, 2022. https://doi.org/10.1016/j.jjimei.2022.100106

[19] H. Aldawood, T. Alashoor, and G. Skinner, "Does awareness of social engineering make employees more secure?," *International Journal of Computer Applications*, vol. 177, no. 38, pp. 45-49, 2020. https://doi.org/10.5120/ijca2020919891

[20] S. H. Bhaharin, U. Asma'Mokhtar, R. Sulaiman, and M. M. Yusof, "Issues and trends in information security policy compliance," presented at the 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS), IEEE., 2019.

[21] M. Zaoui, B. Yousra, S. Yassine, M. Yassine, and O. Karim, "A comprehensive taxonomy of social engineering attacks and defense mechanisms: Toward effective mitigation strategies," *IEEE Access*, vol. 12, pp. 72224–72241, 2024. https://doi.org/10.1109/access.2024.3403197

[22] F. A. M. Yusoff, R. N. R. Yusof, and S. R. Hussin, "Halal food supply chain knowledge and purchase intention," *International Journal of Economics and Management*, vol. 9, no. 1, pp. 155-172, 2015.

[23] A. Al-Okaily, M. Al-Okaily, F. Shiyyab, and W. Masadah, "Accounting information system effectiveness from an organizational perspective," *Management Science Letters*, vol. 10, no. 16, pp. 3991-4000, 2020. https://doi.org/10.5267/j.msl.2020.7.010

[24] J. Hair and A. Alamer, "Partial least squares structural equation modeling (PLS-SEM) in second language and education research: Guidelines using an applied example," *Research Methods in Applied Linguistics*, vol. 1, no. 3, p. 100027, 2022. https://doi.org/10.1016/j.rmal.2022.100027

[25] G. D. Garson, *Partial least squares: Regression and structural equation models*. Asheboro, NC, USA: Statistical Publishing Associates, 2016.

[26] T. Cleff, *Applied statistics and multivariate data analysis for business and economics: A modern approach using SPSS, Stata, and Excel*. Cham, Switzerland: Springer, 2019.

[27] B. Blumberg, D. Cooper, and P. Schindler, *EBOOK: Business research methods*. Maidenhead, UK: McGraw Hill, 2014.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 2954-2963, 2025
DOI: 10.55214/25768484.v9i4.6701