International Journal of Information System & Technology
Akreditasi No. 158/E/KPT/2021 | Vol. 6, No. 5, (2023), pp. 629-636

# The Impact of Employees' Information Security Awareness on Information Security Behaviour

*Melissa Indah Fianty*
*Universitas Multimedia Nusantara, Tangerang, Indonesia*
*Email: melissa.indah@umn.ac.id*

***Abstract***

*Internal threats have been a hot topic in information security for several years. According to a 2018 Insider Threat Reports survey, 51% of users are more concerned about internal carelessness and negligence than 47% about external attacks. The availability of information has a vital role for companies today, including confidentiality and integrity in supporting company performance. Users or employees are an essential factor in many information security breaches. This study aims to determine whether security education & training, information security awareness, employee relations, employee accountability, organizational culture, and national culture significantly affect Information System Security Behavior. The sample of this research is employees who work at PT Infracom Technology. Sampling was carried out using the Likert Scale method, and data collection was carried out using questionnaires distributed directly to employees as many as 72 respondents. The statistical method uses Linear Regression Analysis, with statistical tests to test the hypothesis. The results showed a direct and significant influence between security training and education factors, information security awareness, employee relations, and employee responsibility. The most influential variable was employee accountability.*

***Keywords:*** *Information System Security Behavior, Security Education & Training, Information Security Awareness, Employee Relationships, Employee Accountability*

## 1. Introduction

A data breach is a case of cyber-attack, a condition when hackers can enter the system and extract essential data [1]. In 2020, Indonesia was shocked by the incident of a data leak at Tokopedia, the largest e-commerce platform at that time. Based on data from CNN Indonesia, the leak of 91 million Tokopedia accounts, including 91 million accounts and 7 million merchant accounts, was successfully hacked [2]. The data that was successfully hacked were user ID, email, full name, date of birth, gender, mobile phone number and password that were still hashed or encrypted and were sold on the dark web for US$5,000 or around Rp 74 million. The following is a list of data breach cases that occurred in companies in Indonesia from 2020 to 2021 [3].

The data breaches in Indonesia spread to various companies in several provinces and attacked data security in large companies and government agencies. This makes Indonesia ranked 1st out of 5 countries most vulnerable to cybercrime [4]. The five regions of Indonesia most vulnerable to data breaches are Jakarta, Aceh, West Java, Central Java, and East Java. While the most common type of threat is Trojan malware in the form of a link, usually found on a website, a link is clicked, and the malware will start working by sending all the information the hacker wants [5]. Then the hacker will control the infected system and even commit cybersecurity violations [6]. These facts, website breaches play an essential role in many cases of cyber violations. In 2020, attacks on Web sites accounted for 43% of the total number of cybersecurity breaches.

Information security technology is needed in every media vulnerable to being hacked [7]. Some of the information security technologies that are commonly used are firewalls as barriers between networks, antivirus software to scan and track

ISSN : 2580-7250

malicious files on the network, intrusion detection systems (IDS) to scan and analyze network traffic, access control to check network access, security information and event management (SIEM) to record information about track records or activities that occur in the IT environment [8].

Although there is already technology that can protect information assets, information security is also vulnerable to human-caused breaches [9]. A survey on individual motivations for carrying out internal attacks stated that 57% had the motivation to commit fraud and 50% for monetary gain, followed by intellectual property (IP) theft at 43%. Human negligence can lead to a high risk of system breaches and accidental data leaks [10]. To prevent these things, companies need to establish policies related to information technology and educate their employees [11]. That way, the company can also minimize the occurrence of data breaches [12]

Furthermore, it is also necessary to identify the variables that influence employee security behavior regarding information security in organizational settings using an exploratory research approach [13]. The variables that affect employee security behavior are hacking and malware attacks, top management attention, information security awareness/security training, information security policy and security enforcement [14].

The combination of security countermeasures and cultural factors influences employee behavior in an organization [15]. This study's findings indicate a relationship between organizational culture, national culture, and security countermeasures factors on employee security behavior [16]. Other studies examine the role of top management, organizational culture, and other determinants in shaping employee compliance. It shows that top management, directly and indirectly, impacts employee behavior with security policies. Sampling in this study is a PT Infracom Technology. The variables used in this study are Security Education and Training (SET), Information Security Awareness (ISA), Employee Relationship (ER), Employee Accountability (EA), Organizational Culture (OC), And National Culture (NC) to test its effect on employee security behavior [17].

## 2. Research Methodology

The following is the research model used:

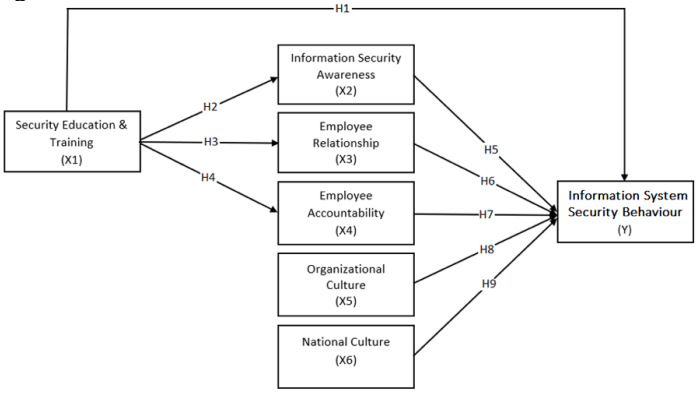


**Figure 1.** Research Model

The research model in figure 1, is a modification of the three previous research models, namely from Yaokumah et al., Connolly et al.. Connolly et al. Hypothesis 1, Hypothesis 3, Hypothesis 4, Hypothesis 6, and Hypothesis 7 were adopted from the model of Yaokumah et al. Hypothesis 2 and Hypothesis 5 were adopted from the model of Connolly et al. Meanwhile, Hypothesis 8 and Hypothesis 9 were adopted from the model of Connolly et al.

Some hypotheses that can be formulated are as follows:

a) H1: Security Education & Training significantly influences Information System Security Behavior.
b) H2: Security Education & Training significantly affects Information Security Awareness.
c) H3: Security Education & Training significantly affects Information Employee Relationship.
d) H4: Security Education & Training significantly affects Employee Accountability.
e) H5: Information Security Awareness significantly influences Information System Security Behavior.
f) H6: Employee Relationship has a significant influence on Information System Security Behavior.
g) H7: Employee Accountability significantly influences Information System Security Behavior.
h) H8: Organizational Culture significantly influences Information System Security Behavior.
i) H9: National Culture significantly influences Information System Security Behavior. Equations

The analytical method used in this research is Structural Equation Modeling (SEM) using SmartPLS 3 software [18]. SEM is a general multivariant analysis technique and is very useful, including unique versions in several other analytical methods as exceptional cases. SEM examines the relationships between variables in a model, be it between indicators and their constructs or relationships between constructs. The SEM model is divided into 2: the measurement and structural models. Validity and reliability tests will be carried out. The validity Test is divided into 2:

1) Convergent Validity Test
   Convergent Validity aims to determine the Validity of each relationship between indicators and their latent constructs or variables. In this study, we want to see the value of the loading factor on each indicator, whose value must be greater than or equal to 0,7.
2) Discriminant Validity Test
   Discriminant validity is carried out to ensure that each concept of each latent model is different from other variables. In this study, the value of Average Variance Extracted (AVE) on each variable must be greater than or equal to 0,5.

A reliability test can be done by calculating Cronbach's Alpha and Composite Reliability values. The test is reliable if Cronbarch's Alpha value is greater than or equal to 0,6 and the Composite Reliability value is greater than or equal to 0,7.

## 3. Results and Discussion

### 3.1. Previous Research

In table 1. The questionnaire results for each variable. After making and distributing questionnaires, 72 respondents were obtained, consisting of staff from various divisions at PT Infracom Technology. The data is then processed using SmartPLS 3 tools to determine the validity and reliability of the data collection results and the relationship between research variables.

**Table 1.** The results of the questionnaire for each variable

| No | Variables | Results |
|---|---|---|
| 1 | Security Education & Training Variable (SET) | It can be concluded that most employees already have sufficient knowledge and have received training in information security. |
| 2 | Information Security | It can be concluded that most employees have |

| No | Variables | Results |
|---|---|---|
| | Awareness Variable (ISA) | awareness and can identify information security in case of a violation. |
| 3 | Employee Relationship Variable (ER) | This proves that most employees of PT. ICT is treated well by the company. Employees are also provided with facilities to accommodate their complaints. The company also helps employees when they experience a big problem by temporarily reducing their responsibilities, and respondents feel that their boss can be invited to communicate well and freely. |
| 4 | Employee Accountability Variable (EA) | It can be concluded that most employees have an information security confidentiality agreement and are willing to report and accept the consequences of an information security violation. |
| 5 | Organizational Culture Variable (OC) | Results can be concluded that most employees are satisfied with the company's environment, but specifically on the OC2 and OC4 indicators, employees tend to be neutral. |
| 6 | National Culture Variable (NC) | This shows that most respondents are neutral towards the unique work environment. Then for NC2, it has a mean of 4.03, where this number indicates that most respondents prefer to work in groups. While NC3 has a mean of 4.29, it shows that the majority of respondents are adaptive to security policies and procedures within the company. |
| 7 | Information System Security Behavior Variable (ISBB) | The mean value of ISSB1 is 4.52, which shows that most respondents comply with the personal information security policy, ISSB2 shows a mean of 3.19 which means that the average employee does not access social media at work, and ISSB3 shows a mean of 4.43 which indicates that the majority of employees use office facilities wisely. |

### 3.2. Convergent Validity Test

Loading factor is a value or coefficient showing the relationship level between the indicator and the latent variable. The variable can be valid if the loading factor value is greater than or equal to 0,7 [19]. Variables have a loading factor value greater than 0.7. However, there are still several invalid variables because they have a loading factor value of less than 0.7, namely the ISSB2, NC1, OC1, OC2, and OC4 variables. Therefore, a second test is needed by eliminating the five variables with a loading factor value of less than 0.7. The results of the second test loading factor value show that all variables are declared valid because they have a loading factor value of more than 0.7. In addition, there is a change in the value of the loading factor on the indicator variables OC3, OC5, OC6, and NC2.

### 3.3. Discriminant Validity Test

Average Variance Extracted (AVE) is a value that evaluates discriminant validity for each construct and latent variable. In this study, the AVE value must be greater than or equal to 0.5 [20].The AVE value is far above the minimum value, so all variables can be said to be valid. Then a discriminant validity test was also carried out based on the Fornell Larcker Criterion. In this test, the correlation value of the variable itself cannot be smaller than the correlation value of the variable with other variables.

**Table 2.** Test Results Based on Fornell Larcker Criterion

| | EA | ER | ISSB | ISA | NC | OC | SET |
|---|---|---|---|---|---|---|---|
| **EA** | 0,87 | | | | | | |
| ER | 0,70 | 0,88 | | | | | |
| ISSB | 0,63 | 0,56 | 0,90 | | | | |
| ISA | 0,85 | 0,69 | 0,67 | 0,88 | | | |
| NC | 0,63 | 0,51 | 0,61 | 0,59 | 0,83 | | |
| OC | 0,75 | 0,78 | 0,65 | 0,63 | 0,59 | 0,87 | |
| SET | 0,84 | 0,72 | 0,52 | 0,79 | 0,55 | 0,63 | 0,91 |

In tabel 2. the Fornell Larcker Criterion results show that each variable has the most significant correlation value with itself than with other variables. After that, a discriminant validity test was carried out based on cross-loadings. In this test, the indicator correlation value of each variable is the largest compared to the correlation of these indicators to other variables. The result of discriminant validity is based on cross-loadings, where it can be seen that each indicator has the most significant correlation value against its variable compared to other variables.

### 3.4. Reliability Test

The reliability test was carried out by calculating Cronbach's Alpha and Composite Reliability values. The test is reliable if Cronbach's Alpha value is greater than or equal to 0,6 and the Composite Reliability value is greater than or equal to 0,7 [21].

**Table 3.** Reliability Test Results Based on Cronbach's Alpha

| Variable | Cronbach's Alpha | Min. Value | Result |
|---|---|---|---|
| Employee Accountability | 0,893 | ≥ 0.6 | Reliable |
| Employee Relationship | 0,905 | ≥ 0.6 | Reliable |
| Information System Security Behavior | 0,905 | ≥ 0.6 | Reliable |
| Information Security Awareness | 0,763 | ≥ 0.6 | Reliable |
| National Culture | 0,590 | ≥ 0.6 | Not Reliable |
| Organizational Culture | 0,838 | ≥ 0.6 | Reliable |
| Security Education Training | 0,927 | ≥ 0.6 | Reliable |

In table 3, it can be seen that the majority of variables have Cronbach's Alpha values greater than 0.6. However, the national culture variable has a Cronbach's Alpha value of less than 0,6, which is only 0,590. Therefore, the national culture variable needs to be more reliable when viewed from Cronbach's Alpha test.

**Table 4.** Reliability Test Results Based on Composite Reliability

| Variable | Composite Reliability | Min. Value | Result |
|---|---|---|---|
| Employee Accountability | 0,93 | ≥ 0.7 | Reliable |
| Employee Relationship | 0,93 | ≥ 0.7 | Reliable |
| Information System Security Behavior | 0,89 | ≥ 0.7 | Reliable |
| Information Security Awareness | 0,93 | ≥ 0.7 | Reliable |
| National Culture | 0,82 | ≥ 0.7 | Reliable |
| Organizational Culture | 0,90 | ≥ 0.7 | Reliable |
| Security Education Training | 0,95 | ≥ 0.7 | Reliable |

In table 4, it can be seen that all variables have Composite Reliability values greater than 0.7. This shows that all variables are said to be reliable based on the Composite Reliability test.

### 3.5. Coefficient of Determination (R2) Evaluation

**Table 5.** Coefficient of Determination (R2) Evaluation

| Variabel | Rsquare | R Square Adjusted |
|---|---|---|
| Employee Accountability | 0,708 | 0,704 |
| Employee Relationship | 0,512 | 0,505 |
| Information System Security Behavior | 0,626 | 0,621 |
| Information Security Awareness | 0,577 | 0,537 |

In tabel 5. shows that the R2 value of the employee accountability variable is 0.708, and the information system security behaviour variable is 0.626, which shows that both variables have strong model interpretation values. Then for the employee relationship variable R2 of 0.512 and information security awareness of 0.577, both variables have moderate model interpretation values.

### 3.6. Hypothesis Testing

Hypothesis testing was carried out using the bootstrapping method [22]. The significance level used is 5%, meaning that the relationship between variables is said to be significant if p-values <0.05 [23]. Table 6. the results of hypothesis testing with p-values.

**Table 6.** Hypothesis Test Results Based on P-values

| Variable Correlation | P-Values | Result |
|---|---|---|
| Security Education & Training -> Information Security Behavior | 0,406 | No significant effect |
| Security Education & Training -> Information Security Awareness | 0,000 | Significant effect |
| Security Education & Training -> Employee Relationship | 0,000 | Significant effect |
| Security Education & Training -> Employee Accountability | 0,000 | Significant effect |
| Information Security Awareness -> Information System Security Behavior | 0,015 | Significant effect |
| Employee Relationship -> Information System Security Behavior | 0,858 | No significant effect |
| Employee Accountability -> Information System Security Behavior | 0,893 | No significant effect |
| Organizational Culture -> Information System Security Behavior | 0,067 | No significant effect |
| National Culture -> Information System Security Behavior | 0,067 | No significant effect |

After performing statistical analysis on each hypothesis, it can be seen that the Employee Accountability variable is the variable that most influences Information System Security Behavior because it has the most considerable R2 value of 0.708, meaning that every 1% increase in the value of the Employee Accountability variable will increase the value of the Information System Security Behavior variable by 0.708 with the assumption that other variables have a fixed value. Based on the research results, the theoretical implications are as follows:

a) The level of employee responsibility greatly influences the employee's behavior towards information system security.

b) Information security Awareness greatly influences the employee's behavior towards information system security.
c) The relationship that an employee can influence the employee's behavior towards information system security.

Then for practical implications, the results of this study will be helpful in the research object company to determine priority factors in terms of creating a work environment free from information security breaches. In addition, the assessment results can also be used to assess the level of security that has been implemented to date and as supporting data to create future information system security training programs.

## 4. Conclusion

This study aims to determine what factors influence Information System Security Behavior or employee behavior at PT Infracom Technology, both factors that influence directly or indirectly (mediated). The conclusion that can be drawn from this research is that four main factors can influence the behavior of users/employees in using the company's information system, which are security education and training, awareness of information security, a strong relationship owned by employees, and level of employee responsibility. Therefore, companies should prioritize the four factors above to improve the quality of internal information security.

## References

[1] M. indah Fianty, A. Angelina, G. Claudia, and D. Sertivia, "Analysis of Factors Affecting Information System Security Behaviour in Employees at IT Company," *Ultima Infosys : Jurnal Ilmu Sistem Informasi*, vol. 13, no. 1, 2022.
[2] Cyberthreat.id, "12 Kasus Kebocoran Data di Indonesia Sejak 2019,"," Nov. 05, 2021.
[3] Kompas, "Lazada Kebobolan, 1,1 Juta Data Pengguna RedMart Diretas," *KOMPAS.com*, Nov. 02, 2020.
[4] Cloud BSSN, "Laporan_Tahunan_Honeynet 2020," Jakarta, 2020.
[5] Michael E. Whitman and Herbert J. Mattord, *Principles of Information Security (MindTap Course List)*, 7th ed. Cengage Learning; 7th edition , 2021.
[6] J. Goo, M.-S. Yim, and D. Kim, "A Path to Successful Management of Employee Security Compliance: An Empirical Study of Information Security Climate," *Professional Communication, IEEE Transactions on*, vol. 57, pp. 286–308, Dec. 2014, doi: 10.1109/TPC.2014.2374011.
[7] M. Alohali, N. Clarke, S. Furnell, and S. Albakri, "Information security behavior: Recognizing the influencers," in *2017 Computing Conference*, 2017, pp. 844–853. doi: 10.1109/SAI.2017.8252194.
[8] L. Zemmouchi-Ghomari, "Basic Concepts of Information Systems," in *Contemporary Issues in Information Systems*, D. Reilly, Ed. Rijeka: IntechOpen, 2021, p. Ch. 2. doi: 10.5772/intechopen.97644.
[9] A. Yuryna Connolly, "Employee Security Behaviour: The Importance of Education and Policies in Organisational Settings," Feb. 2018.
[10] Cybersecurity Insiders, "Insider Threat Report," 2019.
[11] G. Solomon and I. Brown, "The influence of organisational culture and information security culture on employee compliance behaviour," *J. Enterp. Inf. Manag.*, vol. 34, pp. 1203–1228, 2020.
[12] D. C. Islami, K. B. I.H, and C. Candiwan, "Kesadaran Keamanan Informasi pada Pegawai Bank x di Bandung Indonesia," *Jurnal INKOM*, vol. 10, no. 1, p. 19, Nov. 2016, doi: 10.14203/j.inkom.428.

[13] W. Yaokumah, D. Walker, and P. Kumah, "SETA and Security Behavior - Mediating Role of Employee Relations, Monitoring, and Accountability," *Journal of Global Information Management*, vol. 27, pp. 102–121, Apr. 2019, doi: 10.4018/JGIM.2019040106.

[14] N. N. A. Shamsudin, S. F. M. Yatin, N. F. M. Nazim, A. W. Talib, M. A. M. Sopiee, and F. N. Shaari, "Information Security Behaviors among Employees," *International Journal of Academic Research in Business and Social Sciences*, vol. 9, no. 6, Jun. 2019, doi: 10.6007/ijarbss/v9-i6/5972.

[15] A. Yuryna Connolly, M. Lang, and D. Tygar, *Investigation of Employee Security Behaviour: A Grounded Theory Approach*, vol. 455. 2015. doi: 10.1007/978-3-319-18467-8_19.

[16] G. Solomon and I. Brown, "The influence of organisational culture and information security culture on employee compliance behaviour," *Journal of Enterprise Information Management*, vol. 34, pp. 1203–1228, Jul. 2021, doi: 10.1108/JEIM-08-2019-0217.

[17] W. Yaokumah, D. O. Walker, and P. Kumah, "SETA and security behavior: Mediating role of employee relations, monitoring, and accountability," *Journal of Global Information Management*, vol. 27, no. 2, pp. 102–121, Apr. 2019, doi: 10.4018/JGIM.2019040106.

[18] D. L. Sumarna and N. B. Manik, "Analisis Technology Acceptance Model (Tam) Terhadap Pengguna Sap Pt Polychemie Asia Pacific Permai," *Jurnal Logistik Bisnis*, vol. 09, no. 2, 2019, [Online]. Available: http://ejurnal.poltekpos.ac.id/index.php/logistik/index

[19] A. Purwanto and Y. Sudargini, "Partial Least Squares Structural Squation Modeling (PLS-SEM) Analysis for Social and Management Research : A Literature Review," *Journal of Industrial Engineering & Management Research*, vol. 2, no. 4, doi: 10.7777/jiemar.v2i4.

[20] G. TomassMHultt, "Classroom Companion: Business Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R AAWorkbook." [Online]. Available: http://www.

[21] K. S. Taber, "The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education," *Res Sci Educ*, vol. 48, no. 6, pp. 1273–1296, 2018, doi: 10.1007/s11165-016-9602-2.

[22] L. Nikitina, R. Paidi, and F. Furuoka, "Using bootstrapped quantile regression analysis for small sample research in applied linguistics: Some methodological considerations," *PLoS One*, vol. 14, no. 1, pp. e0210668-, Jan. 2019, [Online]. Available: https://doi.org/10.1371/journal.pone.0210668

[23] C. Andrade, "The P value and statistical significance: Misunderstandings, explanations, challenges, and alternatives," *Indian Journal of Psychological Medicine*, vol. 41, no. 3. Wolters Kluwer Medknow Publications, pp. 210–215, May 01, 2019. doi: 10.4103/IJPSYM.IJPSYM_193_19.