ISSN 2085-4579

Analysis of Factors Affecting Information System Security Behaviour in Employees at IT Company

Melissa indah Fianty[1], Aileen Angelina[2],Gavrilla Claudia[3], Devita Sertivia[4], Jevelin[5]
Universitas Multimedia Nusantara, Tangerang, Indonesia
[1] melissa.indah@umn.ac.id, [2]aileen.angelina@student.umn.ac.id, [3]gavrilla.claudia@student.umn.ac.id,
[4]devita.sertivia@student.umn.ac.id, [5]jevelin@student.umn.ac.id

Accepted 10 June 2022
Approved 30 June 2022

***Abstract*— Most companies have prioritized a technology approach to protecting their information assets from potential attacks. The availability of information has a vital role for companies today, including confidentiality and integrity in supporting the company's performance. Users or employees are a significant factor in many information security breaches. This study aims to determine whether security education & training, information security awareness, employee relationships, employee accountability, organizational culture, and national culture significantly affect Information System Security Behavior. The analysis uses survey data from employees at companies in Jakarta and uses a structural equation modeling approach through SmartPLS 3. The results show that there is no direct and significant effect between security education & training on employee security behavior in companies in Jakarta. Security education & training affects the three mediators (Information System Awareness, Employee Relationship, and Employee Accountability), and the three mediators affect employee security behavior. The most influential variable is employee accountability.**

Index Terms—*Information System Security Behavior, Security Education & Training, Information Security Awareness, Employee Relationships, Employee Accountability.*

I. INTRODUCTION

Information Technology is the design, implementation, development, support, and management of computer-based information systems consisting of hardware or software. In this increasingly advanced era, information technology is widely used to efficiently the company's time and operational costs in processing large and substantial amounts of data [1]. The security of data or information owned by the company needs to be considered in the use of information technology. Security is an essential part of information systems because it concerns personal and confidential data belonging to users or companies. However, unfortunately, information system vulnerabilities related to data are still common. Vulnerabilities can occur due to various threats, including viruses, human error, and hacking.

In 2020, the data breach incident became a big topic in Indonesia, where millions of personal data belonging to users on various major e-commerce sites were leaked. One of the essential assets for a company is data, where much information can be used from the data. A data breach incident may result in the disclosure of PII (Personal Identifiable Information) from an individual at risk of theft or misuse of a person's data [2].

Based on the website of the State Cyber and Password Agency (BSSN) in 2021, here are the provinces in Indonesia that experienced the most data breaches from January to December 2021:

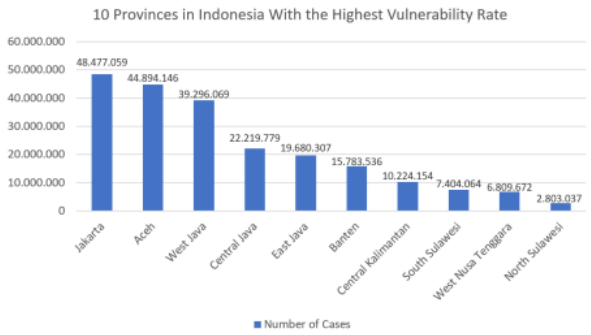

Figure 1. 10 Provinces in Indonesia with the Highest Vulnerability Rate [3]

Based on Figure 1, it can be known that data breach incidents still occur in Indonesia. The province in Indonesia with the highest vulnerability rate in Greater Jakarta province, with 48,477,059 cases.

Meanwhile, in 2021, the Garuda Eye Monitoring System detected 217.7 million cyber threats to Indonesia's internet network. Most of these threats are attempted data leaks using the Malware method [4]. This Malware is a type of ransomware that can encrypt files and directories on an infected computer, and generally, a notification will appear to pay a ransom [5]. The results of reports in 2021 from 99 firms show that 71% of the most common cyber threats are Malware that attacks company databases and blocks user access [6]. One factor that influences the threat of Malware is an element of intent carried out by irresponsible parties and the users' negligence. One example of the failure of the user himself is accidentally accessing a particular site, where the site asks for authentication or notification so that unknowingly, this will give Malware permission to enter and attack the user's computer. Some areas even show a pop-up that triggers the computer to download a file or application, which causes Malware to enter and damage the operating system without the user knowing [7].

Threats in the company are evidence that users/employees still do not have good information security awareness, so without them realizing their activities in using the company network, including the use of the internet, they can pose a threat to the security of company information [8]. Almost all companies have prioritized a technology approach to protecting their information assets from potential attacks. Some commonly used information security technologies include firewall devices, Antivirus software, IDS, and others. Although the prevention of attacks by technical means is essential, on the other hand, the risk of insider threats to information security breaches is genuine. Users or employees are a significant factor in many information security breaches. Thus, more and more attention is paid to the human side of information security [9].

Employees are the leading cause of many data breaches in companies. Information security breaches often occur due to employee ignorance or careless behavior [10]. Based on Nucleus Cyber in the 2019 Insider Threat Report seen in Figure 2, companies are more worried about unintentional/negligent data breaches (70%), data breaches due to negligence (66%), and intentional data breaches (62%).

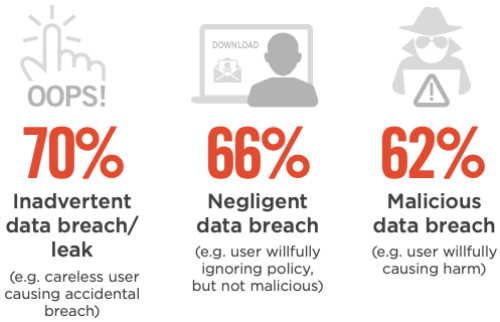

Figure 2. Types of Internal Threats [11]

In the same report in Figure 3, it is explained that the main reason for internal attacks is the lack of awareness and training of employees (56%).

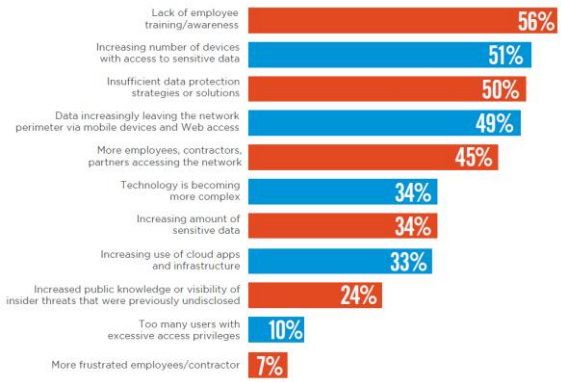

Figure 3. Main Causes of Internal Attacks

Maintaining employee compliance with information security rules is highly dependent on the employees' behavior because technical controls cannot prevent all human errors. For example, employees tend to write down passwords, share them with coworkers, or send confidential information in an unencrypted form. At the same time, other sources say that employees are the weakest link in the information security chain [12]. The main challenge for organizations is to find ways to build employee awareness and concern about the importance of information security.

Based on the Preventive Maintenance report for the period February - April 2022 at one of the IT companies in Jakarta, there are several threats:

Figure 4. Threats in IT Company

Threat	Category	Threat Level	Blocked or Allowed	Number of Incidents
A hack occurs when the old server migrates to a new server.	Brute force	Critical	Blocked	1
There was a leak of customer data.	Deliberate acts of theft.	Critical	Blocked	1

Based on the threats seen in Figure 4, there are still many employees who do not have a high awareness of the importance of information security in the company. As for the risks that occur due to threats to information security, namely, data contained in computer systems can be tampered with or deleted; data can be accessed or changed by the unauthorized user; falsification of information by unauthorized persons [13].

Threats can also occur when accessing a website without guaranteed security. There are several access violations to specific websites with different categories:

Figure 5 Website Breach at an IT Company

URL	Category Description	Action
https://www.netflix.com/browse	Media streaming and downloads entertainment	Blocked
https://web.telegram.org/	Computer & technology, instant messaging, and chat	Blocked

Based on Figure 5, the company blocked Netflix because Netflix was not willing to meet some of the subscription-based videos on demand (SVOD) service requirements applicable to the company [14]. This company also blocks the Telegram website because of the orders given by the Indonesian government [15].

Sampling in this study is a company in Jakarta. 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.

II. METHOD

A. *Research Model*

The following is the research model used:

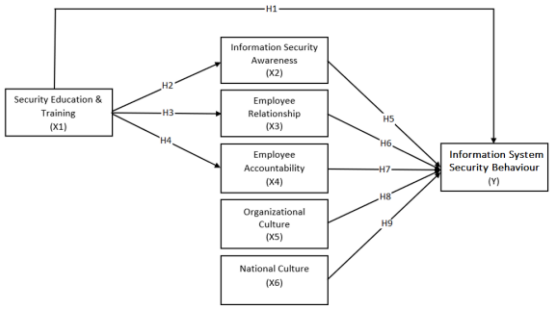

Figure 6 Research Model

The research model in figure 6 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.

B. *Hypothesis*

Some hypotheses that can be formulated are as follows:

- H1: Security Education & Training significantly influences Information System Security Behavior.
- H2: Security Education & Training significantly affects Information Security Awareness.
- H3: Security Education & Training significantly affects Information Employee Relationship.
- H4: Security Education & Training significantly affects Employee Accountability.
- H5: Information Security Awareness significantly influences Information System Security Behavior.
- H6: Employee Relationship has a significant influence on Information System Security Behavior.
- H7: Employee Accountability significantly influences Information System Security Behavior.
- H8: Organizational Culture significantly influences Information System Security Behavior.
- H9: National Culture significantly influences Information System Security Behavior. Equations

C. *Variable Measurement*

In measuring variables, indicators are needed to test the validity of these variables. The indicators obtained are based on three journals in the research model. They will be used to develop questions that are compiled into a questionnaire that will be distributed to respondents [16].

D. *Data collection technique*

The measurement in this study will use a Likert scale where data is collected from the results of a

questionnaire survey which is distributed using a google form and distributed to employees at an IT company in Jakarta.

E. Data analysis

The analytical method used in this research is Structural Equation Modeling (SEM) using SmartPLS 3 software. [17].

- *Measurement Model*

  Because the data collection in this study used a questionnaire, it is necessary to have a measuring tool to determine validity and reliability. A validity test is a form of testing the quality of primary data to measure the validity of a question in research. At the same time, the reliability test is a tool to measure a questionnaire which is an indicator of a variable or constructs. A questionnaire is said to be reliable or reliable if someone's answers are consistent with the questions [18].

  The validity test consists of two types: the convergent validity test and the discriminant validity test. The convergent validity test can be done in several ways, including by looking at the loading factor value on each indicator, whose value must be greater than 0.7 or through the Average Variance Extracted (AVE) value on each variable value must be greater than 0.5.

  The reliability test can be done by calculating the Cronbach's Alpha and Composite Reliability value. The test is reliable if the Cronbach's Alpha value is above 0.6 and the Composite Reliability value is above 0.7.

III. RESULTS AND DISCUSSINS

A. Previous Research

The research model used is a modification of the three previous research models.

- SETA significantly impacts security behaviour through monitoring, ER, and EA [19].
- The journal Employee Security Behaviour shows that security procedures such as rules and education impact employees' awareness to behave obediently [20].
- The journal Investigation of Employee Security Behavior investigates security precautions and cultural factors against employee security behaviour [21].
- The journal Managing Employee Compliance with IS Policies discusses three variables: Top Management, Organizational Behavior, and Theory of Planned Behavior [22].
- The journal The Influence of Organisational Culture and Information Security Culture on Employee Compliance Behavior discusses the combined influence of OC and information security culture [23].

B. The Convergent Validity Test

An indicator must represent one latent variable and underlie the latent variable. For this reason, a convergent validity test is needed. The convergent validity test can be done in several ways, including looking at the loading factor value, which is the value generated by each indicator to measure the variable, or the Average Variance Extracted (AVE) value. In this study, the loading factor value must be greater than 0.7, and the Average Variance Extracted (AVE) value must be greater than 0.5. This value describes adequate convergent validity, which means that one latent variable can explain more than half of the variance of its indicators on average.

- H1: Security Education & Training significantly influences Information System Security Behavior.

  Values of Outer Loadings: There is still a loading factor value smaller than 0.7, namely SET1 with a value of 0.306, SET2 with a value of 0.268, and SET3 with a value of 0.247 and Cronbach's Alpha Value: there are still Average Variance Extracted (AVE) values smaller than 0.5, such as latent variable 1.
- H2: Security Education & Training significantly affects Information Security Awareness.

  Values of Outer Loadings: there is still a loading factor value smaller than 0.7, namely SET4 with a value of 0.473 and Cronbach's Alpha Values: it can be seen that latent variable one and latent variable 2 have an AVE value greater than 0.5.
- H3: Security Education & Training significantly affects Information Employee Relationship.

  Values of Outer Loadings: There are still loading factor values smaller than 0.7, namely ER4 with a value of 0.636, SET1 with a value of 0.553, SET2 with a value of 0.431, and SET3 with a value of 0.431. Value 0.454 and Cronbach's Alpha Values: there are still AVE values smaller than 0.5, such as latent variable 1.
- H4: Security Education & Training significantly affects Employee Accountability.

  Values of Outer Loadings: there is still a loading factor value smaller than 0.7, namely EA3 with a value of 0.592 and SET4 with a value of 0.454 and Cronbach's Alpha Values: the AVE values of latent variable one and latent variable 2 are more significant than 0.5.
- H5: Information Security Awareness significantly influences Information System Security Behavior.

  Values of Outer Loadings: there is still a loading factor value smaller than 0.7, namely ISSB2 with a

value of 0.685 and Cronbach's Alpha Values: latent variable one and latent variable 2 have an AVE value greater than 0.5.

- H6: Employee Relationship significantly influences Information System Security Behavior.

  Values of Outer Loadings: there are still loading factor values smaller than 0.7, namely ER4 with a value of 0.349 and ISSB1 with a value of 0.455 and Cronbach's Alpha Values: latent variable one and latent variable 2 have an AVE value greater than 0.5.
- H7: Employee Accountability significantly influences Information System Security Behavior.

  Values of Outer Loadings: there are still loading factor values smaller than 0.7, namely EA3 with a value of 0.697 and ISSB2 at 0.542 and Cronbach's Alpha Values: it can be seen that latent variable one and latent variable 2 have an AVE value greater than 0.5.
- H8: Organizational Culture significantly influences Information System Security Behavior.

  Values of Outer Loadings: there is still a loading factor value smaller than 0.7, namely OC1 with a value of 0.642 and Cronbach's Alpha Values: latent variable one and latent variable 2 have an AVE value greater than 0.5.
- H9: National Culture significantly influences Information System Security Behavior. Equations

Values of Outer Loadings: there are still loading factor values smaller than 0.7, namely ISSB2 with a value of 0.683, NC1 with a value of 0.100, NC2 with a value of 0.606 and Cronbach's Alpha Values, and there are still AVE values smaller than 0.5, such as latent variable 1

C. The Discriminant Validity Test

The result of the Fornell-Larcker Criterion on each variable. That there are two variables whose correlation value on the variable itself is smaller than with other variables, the NC variable with a value of 0.670 and OC with a value of 0.753. Meanwhile, other variables have the most significant correlation value with themselves.

Discriminant validity test based on cross-loadings values. All EA variable indicators have the most significant cross-loadings value (0.735-0.854) in EA constructs. All ER variable indicators have the most significant cross-loadings value (0.629-0.903) in the ER construct. ISA variable indicators have the most significant cross-loadings value (0.715-0.884) in ISA constructs. All ISSB variable indicators have the most significant cross-loadings value (0.661-0.825) in the ISSB construct. The NC variable has one small cross-loadings value in the NC construct, namely the NC1 indicator with a value of -0.072. Meanwhile, the other two indicators have the most significant cross-loading values in NC construction, with values of 0.733 and 0.898. All OC variable indicators have the most significant cross-loadings value (0.656-0.855) in OC constructs. The SET variable has one small cross-loadings value in the SET construct, namely the SET4 indicator with a value of 0.484. Meanwhile, the other three indicators have the most significant cross-loading values in the SET construct with values of 0.732, 0.811, and 0.831.

D. The Reliability Test

Reliability test results can be said to be reliable if Cronbach's Alpha value is above 0.6 and the composite reliability value is above 0.7. Here are the results of reliability tests based on Cronbach's Alpha and Composite Reliability.

- The reliability test result is based on Cronbach's Alpha values on hypotheses 1, 2, 3, and 4. All variables, namely EA, ER, ISA, ISSB, and SET, can be reliable because Cronbach's Alpha values are more than 0.6, namely 0.816, 0.822, 0.827, 0.629, and 0.689.
- The result of a reliability test based on composite reliability values in hypotheses 1, 2, 3, and 4. EA, ER, and ISA variables can be said to be reliable because the Composite Reliability value is more than 0.7. Meanwhile, the ISSB and SET variables are unreliable because the Composite Reliability value is smaller than 0.7.
- The reliability test result is based on Cronbach's Alpha value in hypothesis 5. The ISA and ISSB variables can be said to be reliable because the value of Cronbach's Alpha is more significant than 0.6.
- The reliability test result is based on the Composite Reliability value in hypothesis 5. Isa and ISSB variables can be said to be reliable because the Composite Reliability value is more than 0.7.
- The reliability test result is based on Cronbach's Alpha value in hypothesis 6. The ER and ISSB variables can be said to be reliable because Cronbach's Alpha value is more significant than 0.6.
- The reliability test result is based on the Composite Reliability value in hypothesis 6. ER and ISSB variables can be said to be reliable because the Composite Reliability value is more than 0.7.
- The reliability test result is based on Cronbach's Alpha value in hypothesis 7. The EA and ISSB variables can be said to be reliable because Cronbach's Alpha value is more significant than 0.6.
- The reliability test result is based on the Composite Reliability value in hypothesis 7. EA and ISSB variables can be said to be reliable because the Composite Reliability value is more

- The reliability test result is based on Cronbach's Alpha value in hypothesis 8. The ISSB and OC variables can be said to be reliable because Cronbach's Alpha value is more significant than 0.6.
- The reliability test result is based on the Composite Reliability value in hypothesis 8. ISSB and OC variables can be said to be reliable because the Composite Reliability value is more than 0.7 The reliability test result is based on Cronbach's Alpha value in hypothesis 9. The ISSB variable can be said to be reliable because Cronbach's Alpha value is more significant than 0.6. Meanwhile, the NC variable is not said to be reliable because Cronbach's Alpha value is smaller than 0.6
- The reliability test result is based on the Composite Reliability value in hypothesis 9. The ISSB variable can be said to be reliable because its Composite Reliability value is more than 0.7. Meanwhile, the NC variable is unreliable because the Composite Reliability value is smaller than 0.7.

E. Evaluasi Coefficient of Determination (R2)

The result of the evaluation of the coefficient of determination, where it can be concluded that:

- SET affects EA by 0.485 with an adjusted value of R Square of 0.466. From these results, SET affects EA by 0.466 or 46.6%, and the influence of SET on EA is moderate.
- SET affects the ER by 0.300 with an adjusted value of R Square of 0.275. From these results,
- SET affects the ER by 0.275 or 27.5%, and the influence of SET on ER is moderate.
- SET affects the ISA of 0.586 with an adjusted value of R Square of 0.571. From these results, SET affects the ISA by 0.571 or 57.1%, and the effect of SET on ISA is strong.
- SET, ISA, ER, EA, OC, and NC affect ISSB by 0.729 with an adjusted value of R Square of 0.659. From these results, SET, ISA, ER, EA, OC, and NC affect ISSB by 0.659 or 65.9%, and tthe influence of SET, ISA, ER, EA, OC, and NC on ISSB is strong.

F. The Hypothesis Test

Hypothesis analysis is carried out using bootstrapping methods. The significance level used is 5% (0.05), which means that the relationship between variables is said to be significant if the p-values < 0.05.

Table 4. Hypothesis Test Results Using Bootstrapping

Variable Relationships	β	P-Values	Result
SET → ISSB	-0.061	0.939	No significant effect
SET → ISA	0.765	0.000	Significant effect
SET → ER	0.548	0.032	Significant effect
SET → EA	0.696	0.003	Significant effect
ISA → ISSB	-0.371	0.245	No significant effect
ER → ISSB	0.018	0.936	No significant effect
EA → ISSB	0.340	0.415	No significant effect
OC → ISSB	0.359	0.276	No significant effect
NC → ISSB	0.566	0.054	No significant effect

Table 4 is the result of a hypothesis test using the bootstrapping method. The results of the hypothesis test are based on the following p-values:

- Hypothesis Analysis 1 (H1)
  The hypothesis 1 (H1) test results, namely the influence of the Security Education & Training variable on Information System Security Behavior, obtained a p-value of > 0.05, which is 0.939. Thus, H1 was declared rejected.
- Hypothesis 2 (H2) Analysis
  The results of hypothesis 2 (H2) test, namely the influence of the Security Education & Training variable on Information System Awareness, obtained a p-value of < 0.05, which is 0.000. Thus, H2 is declared accepted.
- Hypothesis Analysis 3 (H3)
  In hypothesis 3 (H3) test results, the influence of the Security Education & Training variable on the Information Employee Relationship obtained a p-value of < 0.05, which is 0.032. Thus, H3 is declared accepted
- Hypothesis Analysis 4 (H4)
  The hypothesis 4 (H4) test results, namely the influence of the Security Education & Training variable on Employee Accountability, obtained a p-value of > 0.05, which is 0.003. Thus, H4 is declared accepted.
- Hypothesis Analysis 5 (H5)
  The results of hypothesis 5 (H5) test, namely the influence of the Information Security Awareness variable on Information System Security Behavior, obtained a p-value of > 0.05, which is 0.245. Thus, H5 is declared rejected.
- Hypothesis Analysis 6 (H6)

The hypothesis 6 (H6) test results, namely the influence of employee relationship variables on Information System Security Behavior, obtained a p-value of > 0.05, which is 0.936. Thus, H6 was declared rejected.

- Hypothesis Analysis 7 (H7)
  The results of hypothesis 7 (H7) test, namely the influence of the Employee Accountability variable on the Information System Security Behavior, obtained a p-value of > 0.05, which is 0.415. Thus, H7 was declared rejected.
- Hypothesis Analysis 8 (H8)
  The hypothesis 8 (H8) test results, namely the influence of the Organization Culture variable on the Information System Security Behavior, obtained a p-value of > 0.05, which is 0.276. Thus, H8 was declared rejected.
- Hypothesis 9 (H9) Analysis
  The results of the hypothesis 9 (H9) test, the influence of National Culture variables on Information System Security Behavior, obtained a p-value of > 0.05, which is 0.054. Thus, H9 was declared rejected.

IV. Conclusion

This study aims to determine what factors influence Information System Security Behavior or employee behavior at IT companies in Jakarta in using company information systems, both factors that influence directly or indirectly (mediated). The conclusions that can be drawn from this research are:

- The National Culture variable is the variable that most influences Information System Security Behavior because it has the most significant value of 0.054, meaning that every increase in the value of the National Culture variable by one unit will increase the value of the Information System Security Behavior variable by 56.6%, assuming other variables is a fixed value.
- Security Education & Training variable has a significant effect on Information System Awareness following the theoretical implications in the last journal, where education, training, and information security awareness are three interrelated organizational activities to encourage employee understanding and compliance with information security and policies. Guidelines.
- Security Education & Training variable has a significant effect on Employee relationships, following the theoretical implications in the last journal, where there is a significant relationship between the Employee Information Security Education & Training variable and the development of Employee relationships.
- Security Education & Training variable has a significant effect on Employee Accountability, following the theoretical implications in the last journal where there is a significant relationship between Employee Information Security Education & Training and Employee Information Security Accountability.

The results of this study can practically be used as input for companies to pay more attention to education, training, and information security awareness of employees. This is because there has been a significant influence between the Security Education & Training variables on Information System Awareness, Employee Relationships, and Employee Accountability

References

[1] [1] Simarmata, J., et al. (2020). Information Technology and Management Information Systems. Our Writing Foundation.

[2] Neto, N. N., Madnick, S., Paula, A. M. G. D., & Borges, N. M. (2021). Developing a global data breach database and the challenges encountered. Journal of Data and Information Quality (JDIQ), 13(1), 1-33.

[3] BSSN, (2021). Honeynet Project Report on Cyber Attack Map, [Online]. Available: https://honeynet.bssn.go.id/

[4] BSSN, " Report from the national monitoring system Mata Garuda," 2019. [Online]. Available: https://bssn.go.id/wp-content/uploads/2019/02/Rilis-Forum-Cyber-Corner- Launching-Honeynet-Project-Revisi.pdf.

[5] BSSN, " BSSN Honeynet Project 2020 Annual Report," 2020. [Online]. Available: https://cloud.bssn.go.id/s/q5Hx6ifSj86cKnA.

[6] 99firm, "Cyber Threat" [Online]. Available: https://99firms.com/.

[7] M. E. Whitman dan H. J. Mattord, "Principles of Information Security," in Information Security Professionals, USA, United States of America, 2021.

[8] J Connolly, L., Lang, M., & Tygar, J. D., "Investigation of employee security behaviour: A grounded theory approach," IFIP Advances in Information and Communication Technology, vol. 455, p. 283-296, 2015.

[9] J. Abawajy, "User preference of cyber security awareness delivery methods," Behaviour & Information Technology, vol. 33, p. 237-248, 2014.

[10] K. Marett, "hecking the manipulation checks in information security research," Information & Computer Security. .

[11] N. Cyber, "Insider Threat Report 2019," Nucleus Cyber, 2019. [Online]. Available: https://nucleuscyber.com/wp-

content/uploads/2019/07/2019_Insider-Threat-Report_Nucleus_Final.pdf.

[12] Whitman, M. E., & Mattord, H. J. (2012). Principles of Information Security Fourth Edition. Course Technology, Cengage Learning.

[13] Sari, I. Y., et al. (2020). Data and Information Security. Our Writing Foundation.

[14] Yaokumah, W., Walker, D. O., & Kumah, P. (2019). SETA and security behavior: Mediating role of employee relations, monitoring, and accountability. Journal of Global Information Management (JGIM), 27(2), 102-121.

[15] Connolly, L. Y., Lang, M., & Tygar, D. J. (2018). Employee security behaviour: The importance of education and policies in organisational settings. Advances in Information Systems Development, 79–96. doi:10.1007/978-3-319-74817-7_6

[16] Princess, A. E. (2019). Evaluation of counseling guidance programs: a literature study. Indonesian Counseling Guidance Journal, 4(2). 39-42.

[17] Sumarna, D. L., & Manik, N.B. (2019). Technology acceptance model (tam) analysis of SAP users of PT Polychemie Asia Pacific Permai. Journal of Business Logistics, 9(02). 68-75.

[18] Sahara, R., Prastiawan, H., & Rizal, D. (2017). Design a Website-Based Telkomsel Mylibrary Information System (Case Study: PT. Cellular Telecommunications). Journal Format, 6(1), 106-118.

[19] Yaokumah, W., Walker, D. O., & Kumah, P. (2019). SETA and security behavior: Mediating role of employee relations, monitoring, and accountability. Journal of Global Information Management (JGIM), 27(2), 102-121.

[20] Connolly, L. Y., Lang, M., & Tygar, D. J. (2018). Employee security behaviour: The importance of education and policies in organisational settings. Advances in Information Systems Development, 79–96. doi:10.1007/978-3-319-74817-7_6

[21] Connolly, L., Lang, M., & Tygar, J. D. (2015). Investigation of employee security behaviour: A grounded theory approach. IFIP Advances in Information and Communication Technology. doi:10.1007/978-3-319-18467-8_19

[22] Alohali, M., Clarke, N., Furnell, S., & Albakri, S. (2017). Information security behavior: Recognizing the influencers. 2017 Computing Conference. doi:10.1109/sai.2017.8252194

[23] Solomon, G & Brown, I. (2019). The Influence of Organisational Culture and Information Security Culture on Employee Compliance Behaviour. Journal of Enterprise Information Management, ISSN: 1741-0398.