UNDERSTANDING EMPLOYEE SECURITY BEHAVIOR IN USING INFORMATION SYSTEM OF ORGANIZATIONS: EVIDENCE FROM JAKARTA GREATER AREA, INDONESIA

RIDIPURNOMO[1], RIYANTO JAYADI[2]
Information Systems Management Department, BINUS Graduate Program — Master of
Information System Management,
Bina Nusantara University, Jakarta, Indonesia
[1]ridipurnomo@binus.ac.id, [2]riyanto.jayadi@binus.edu,

ABSTRACT

Almost all organizations currently have implemented the use of technology in running their business to enhance productivity and performance, there by gaining competitive advantage and achieving strategic goals. However, the use of this technology is very vulnerable to data breaches. Data breach incidents became a big topic in Indonesia during 2020 since the leaks of millions of users' personal data from some of the largest e-commerce sites. This incident should certainly be a warning to all organizations, especially in Jakarta Greater Area (Jabodetabek), Jakarta, Indonesia, to pay more attention to the security of their company's information. Most of organizations have prioritized a technology approach to protect their information assets from potential attacks. Some of the commonly used information security technologies are firewall devices, Antivirus software, IDS, etc. Although the prevention of attacks by technical means is important, the risk of insider threats must be taken into account, Users or employees tend to be the main factor in many information security breaches. This research aims to determine whether security education & training, information security awareness, employee relationships, employee accountability, organizational culture, and national culture have a significant effect on employee security behavior. The empirical analysis relies on a survey data from a cross section of employees from 10 companies in Jabodetabek and a structural equation modeling approach via SmartPLS 3. The results showed no direct and significant effect of security education & training on improving employee security behavior in Jabodetabek. The security education & training influences all mediators (information security awareness, employee relationship and employee accountability), and all the mediators influences employee behavior in using the company's information system. The most influential variable is employee accountability. Organizational culture and national culture influence employee behavior in using company information systems.

Keywords: *Data Breach, Employee Security Behavior, Security Education & Training, Information Security Awareness, Employee Relationships, Employee Accountability, Organizational Culture, National Culture*

1. INTRODUCTION

In this modern era, almost all organizations have implemented the use of technology in running their business to enhance productivity and performance, there by gaining competitive advantage and achieving strategic goals. However, the use of this technology is very vulnerable to data breaches.

Data breach incidents became a big topic in Indonesia during 2020 since the leaks of millions of users' personal data from some of the largest e-commerce sites. Based on the results of the BSSN (Badan Siber dan Sandi Negara) report [1], there were 4 major e-commerce that experienced data breaches, namely Tokopedia (91,000,000 data), RedDoorz (5,800,000 data), Cermati (2,900,000 data) and Kredit Plus (890,000 data). This incident should certainly be a warning to all organizations, especially in Jakarta Greater Area (Jabodetabek), to pay more attention to the security of their company's information.

Most of organizations have prioritized a technology approach to protect their information assets from potential

attacks. Some of the commonly used information security technologies are firewall devices, Antivirus software, IDS, etc. Although the prevention of attacks by technical means is important, the risk of insider threats must be taken into account, Users or employees tend to be the main factor in many information security breaches [2]. Thus, more and more attention is paid to the human side of information security [2].

Employees are the leading source of many data breaches in enterprises, according to the Ponemon Institute (2012). Employee illiteracy or carelessness are common causes of data security breaches in businesses [2]. Nucleus Cyber in its 2019 Insider Threat Report shows that the companies are more concerned about inadvertent data breaches/leak (70%), negligent data breaches (66%), and malicious data breaches (62%). in the same report, the main reason for these internal attacks was due to lack of awareness and training of employees (56%).

Maintaining employee compliance with information security policies depends on the behavior of the employees themselves, as technical controls cannot prevent all human errors. For example, employees tend to write down passwords, share them with others, or send confidential information unencrypted.

Other sources say that employees are the weakest link in the information security chain [4]. The main challenge for organizations is to find ways to build employee awareness about the importance of information security.

Based on some of the existed previous researches, quite a lot of them use several variables taken from structural equation modeling (SEM) as done by Winfred Yaokumah & Walker [5], where the variables tested are Security education, employee relations, employee monitoring, employee accountability and Employee Security Behavior. Qing Hu [6] with the same research model tested organizational culture, national culture, and security countermeasures variables on their effect on employee security behavior variables. Another research was conducted by Dian Chisva Islami, Khodijah Bunga IH and Candiwan [7] regarding Information Security Awareness of Bank X Employees in Bandung, and many of the other existed theories. Another factors were found, such as employee security awareness and information security policy which are suspected to have a significant influence on employee security behavior.

This paper introduces an extended SEM model by taking several variables, including security education, accountability, security awareness, employee relations, organizational culture and national culture, to prove that these factors can improve employee security behavior.

This research cannot be applied universally because every country has a different culture that influences their social behavior, such as individualism and collectivism. Indonesia is a country with eastern culture where people like to work together. Jakarta greater area is the center of Indonesia's main business and economic activity, where almost all of the company's headquarter are located here.

2. LITERATURE RIVIEW

2.1 Employee Security Behavior

Employee security behavior is described as how employees use corporate information systems (hardware, software, network systems, and so on), and it might have security ramifications [8]. How employees handle passwords, how they handle organizational data, and how they use network resources are all examples of employee security practices [8], "interest" behavior includes compliant behavior (i.e. complying with policies, procedures, and organizational norms in relation to information security) and non-compliant behavior (i.e. "deliberate" but non-malicious employee behavior that can harm the organization's information system and lead to non-compliance with policies, procedures and organizational norms in relation to information security).

2.2 Information Security Awareness

Information security awareness is defined by Bulgurcu et al. [9] as "workers' knowledge and comprehension of potential problems linked to information security, the repercussions, and what needs to be done to address security-related concerns." Employees with security awareness are aware of the organization's security practices and rules, as well as their responsibilities in relation to organizational information resources and the consequences of their misuse, which can include a loss of reputation, significant financial loss, and even complete business disruption. Employees who understand the purpose of the organization's security requirements are more likely to follow the rules [9]. Additionally, Bulgurcu, et al. [9] and Straub & Welke [10] stress the importance of user security awareness in encouraging compliance behavior. Procedure security countermeasures are significant organizational artifacts that raise employee knowledge of potential security vulnerabilities and the repercussions of deception [10]. Finally, increasing awareness has a beneficial impact on security behavior because employees are more aware of the need of adhering to company information security policies [9].

2.3 Organizational Culture

Organizational culture, according to Tsui et al. [11], is "a collection of core values held by members of an organization." "A set of artifacts, values, and assumptions that develop from the interactions of organizational members" is how organizational culture is defined [12].

Interactions result in the formation of social order or organizational communication. As a result, symbols, messages, and meanings help to maintain a constant flow of communication in the workplace. This is why it is frequently claimed that an organization is culture rather than a culture that exists within an organization [13]. OC has been demonstrated to have an effect on behavior in previous studies. Kilmann [14] defines culture as a separate and hidden factor that governs organizational behavior and attitudes.

2.4 National Culture

National Culture is defined by Ali and Brooks [15] as a set of essential beliefs, conventions, and shared practices that impact individual behavior in a society. Several academic studies have shown that NC has an impact on organizational behavior. Hofstede [16] contends that national culture binds organizations and highlights cross-national disparities in the operation of organizations and the people who work within them.

2.5 Security education & training

Education, training, and user awareness are all key parts of dealing with human factors and competence in information security. Security education is a method of ensuring that staff are aware of the importance of data security [17]. Information security awareness and training activities, according to McCrohan, Engel, and Harvey [18], will increase security behavior.

2.6 Employee Accountability

Accountability is defined as a quality in which a person is willing to accept responsibility for their actions [19]. It is a process in which a person may be required to explain his or her acts to a third party who has the authority to judge the action and subject the individual to possible repercussions [19]. The perception of accountability, according to Zaman and Saif [20], has a substantial positive association with job performance because it can affect behavior at work.

2.7 Employee Relationship

Employee relations, according to Gennard and Judge [21], is the study of the rules, regulations, and agreements used to manage employees individually and collectively in order to acquire employee commitment to achieving organizational goals and objectives. It is critical to address human behavior and organizational concerns in order to assure information system security [22].

2.8 Hypothesis Development

User education, training, and awareness are critical parts of dealing with human factors and competence in information

security. Security education is a method of ensuring that staff are aware of the importance of data security [17]. Connolly et al. [23] discovered a link between security education and employee relations, as well as

security education and employee accountability, in their research. This study presents the following hypothesis based on these past studies:

H1: Security Education & Training has a significant effect on Employee Security Behavior.
H2: Security Education & Training has a significant effect on Information Security Awareness.
H3: Security Education & Training has a significant effect on Information Employee Relationship.
H4: Security Education & Training has a significant effect on Employee Accountability.

Yaokumah and Walker discovered a link between employee accountability and security behavior in their research. Employees who understand the purpose of the organization's security requirements are more likely to follow the rules [9]. Employees' job achievements are determined by social contact between employers and workers, according to Sivalogathasan & Hashim [24]. This study presents the following hypothesis based on these past studies:

H5: Information Security Awareness has a significant effect on Employee Security Behavior.
H6: Employee Relationship has a significant effect on Employee Security Behavior.
H7: Employee Accountability has a significant effect onEmployee Security Behavior.

Organizational culture (OC) has been found to influence behavior in previous studies. Kilmann [14], for example, defines culture as a separate and hidden factor that governs organizational behavior and attitudes. Connolly et al. [25] discovered a link between organizational culture and security behavior, as well as between country culture and security behavior, in their research. This study presents the following hypothesis based on these past studies:

H8: Organizatinal Culture has a significant effect on Employee Security Behavior.
H9: National Culture has a significant effect on Employee Security Behavior.

Based on these hypotheses, Figure 1 shows the constructed research model in this study. The research model is a modification of the three models in previous research, namely Yaokumah at al. [4], Connoly at al. [25], and Connolly at al. [23].

3. RESEARCH METHODOLOGY

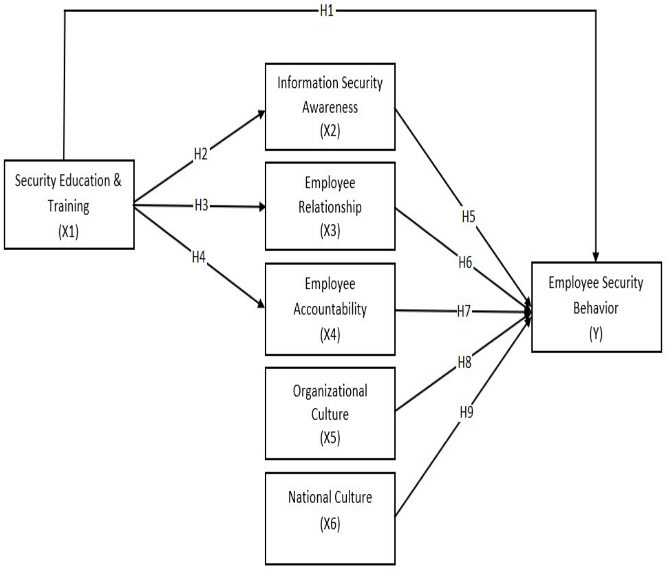
H1
Information Security Awareness (X2)
Employee Relationship (X3)
Employee Accountability (X4)
Organizational Culture (X5)
National Culture (X6)
Security Education & Training (X1)
H2
H3
H4
H5
H6
H7
H8
H9
Employee Security Behavior (Y)

Figure 1: Research Model

3.1 Survey

Respondent data was collected in this study by delivering online surveys using Google Forms to a cross-section of employees from ten organizations in the Jakarta Greater Area (Jabodetabek), Indonesia.

Jabodetabek is Indonesia's largest and most strategically important urban area. Jakarta, Indonesia's capital city, is part of Jabodetabek, which also includes Bogor City, Bogor Regency, Depok City, Tangerang City, South Tangerang City, Tangerang regency, Bekasi City, and Bekasi Regency. With a population of over 27 million people, this metropolis has become a hub of economic activity, accounting for about 22% of the national gross product in 2010.

The questionnaires were distributed through email and Whatsapp. The Measurement using the Likert scale from 1 to 5, where 1 represents "strongly disagree" and 5 represents "strongly agree”.

3.2 Sampling

With million of workers in jabodetabek (Kemnaker, 2021), the sample to be taken in this study is 400 respondents from 10 companies in Jabodetabek with error tolerance 5% and confidence level 95%.

3.3 Respondents Demographics

In this study, the age classification is divided into 6 parts, namely 17-25 years, 26-35 years, 36-45 years, 46-55 years, 5656-65 years, and over 65 years. The results show that the most respondents is from the age 26 - 35 (38.7%), followed by age 17 – 25 (24.9%), age 36 - 45 (24.2%), age 46 – 55 (11.1%), age 56 - 65 (1%), and there were no respondent over 65 years old. Meanwhile, the results of respondents based on gender showed that the majority of respondents were male (58.1%) while the rest were female (41.9%). Then, the results of respondents based on industrial sector showed that the most respondents were oil and gas (24.8%), followed by Others (24.5%), IT (22.3%), finance (14%), health (13.7%), and manufacturing (11%).

Table 1. Sample Characteristic

Respondents	No. of Questionnaire Received	Percent (%)
Industry Sector		
IT Companies	91	22.3
Health Care	56	13.7
Oil and Gas	101	24.8
Financial institution	57	14
Manufacturing	45	11
Others	59	14.5
Gender		
Man	234	58.1
Woman	169	41.9
Age (Years)		
17 – 25	103	24.9
26 – 35	160	38.7
36 – 45	100	24.2
46 – 55	46	11.1
56 - 65	4	1
> 65	0	0

3.4 Validity and Reliabilit

3.4.1 Validity

SmartPLS 3 is used in this study to process the data [26]. A validity test is used to determine whether or not a dataset contains a valid questionnaire. Convergent and discriminant validity are used to conduct this testing. Convergent validity is used to demonstrate that a relationship or correlation between two objects in a model is in fact connected or correlated, and that the results reflect whether or not the model is highly dependable. To declare an indicator legitimate, the convergent validity must be established, which can be done by starting with factor loadings more than 0.7 or Average Variance Extracted (AVE) values greater than 0.5.

Table 2. Outer Loading Data Result

Indicator	Outer Loadings value	Result
Security Education & Training		
SET1	0.853	Valid
SET2	0.888	Valid
SET3	0.875	Valid
SET4	0.901	Valid
Information Security Awareness		
ISA1	0.722	Valid
ISA2	0.763	Valid
ISA3	0.769	Valid
ISA4	0.886	Valid
Employee Relationship		
ER1	0.711	Valid
ER2	0.799	Valid
ER3	0.773	Valid
ER4	0.794	Valid
Employee Accountability		
EA2	0.812	Valid
EA3	0.744	Valid
EA4	0.805	Valid
Organizational Culture		
OC1	0.761	Valid
OC2	0.820	Valid
OC4	0.814	Valid
OC6	0.761	Valid
National Culture		
NC3	1.000	Valid
Employee Security Behavior		
ESB1	0.827	Valid
ESB2	0.799	Valid
ESB3	0.830	Valid

Table 3. Average Variance Extracted Data Result

Contruct	AVE	Result
Employee Accountability	0.621	Valid
Employee Relationship	0.593	Valid
Employee Security Behavior	0.670	Valid
Information Security Awareness	0.578	Valid
National Culture	1.000	Valid
Organizational Culture	0.638	Valid
Security Education & Training	0.773	Valid

Table 2 demonstrates that all indicators have an outer loading value larger than 0.7, and Table 3 shows that all variables have an AVE value greater than 0.5, indicating that they are all genuine indicators and variables. However, five indicators were removed from the prior loadings factor computation, namely EA1, NC1, NC2, OC3, and OC5, because their values were less than 0.7.

The discriminant validity test uses two ways, first, with Fornell Larcker Criterion value. The correlation value against the variable itself cannot be less than the variable's The Fornell Larcker Criterion value is used in the discriminant validity test in one of two ways. The correlation value against the variable must be greater than the correlation value between the variable and other variables. Second, when using Cross Loading, the correlation value of each variable's indicator must be higher than the correlation value of these indicators to other variables. Tables 4 and 5 provide the results, which show that for each variable and indicator, all Fornell Larcker Criterion and Cross Loading values are legitimate.

Table 4. Fornell Larcker Criterion Data Result

	EA	ER	ESB	ISA	NC	OC	SET
EA	**0.788**						
ER	0.737	**0.770**					
ESB	0.714	0.645	**0.819**				
ISA	0.582	0.543	0.547	**0.761**			
NC	0.407	0.416	0.438	0.422	**1.000**		
OC	0.739	0.733	0.678	0.525	0.413	**0.799**	
SET	0.377	0.370	0.360	0.698	0.252	0.374	**0.879**

Table 5. Cross Loadings Data Result

	EA	ER	ESB	ISA	NC	OC	SET
EA2	0.812	0.637	0.617	0.482	0.396	0.630	0.266
EA3	0.744	0.546	0.510	0.451	0.293	0.525	0.291
EA4	0.805	0.557	0.558	0.443	0.271	0.587	0.337
ER1	0.463	0.711	0.421	0.369	0.284	0.548	0.256
ER2	0.606	0.799	0.538	0.462	0.358	0.616	0.327
ER3	0.534	0.773	0.468	0.402	0.321	0.524	0.278
ER4	0.649	0.794	0.547	0.432	0.311	0.565	0.275
ESB1	0.620	0.555	0.827	0.478	0.368	0.615	0.309
ESB2	0.599	0.528	0.799	0.447	0.428	0.510	0.291
ESB3	0.528	0.496	0.830	0.413	0.272	0.534	0.280
ISA1	0.289	0.330	0.308	0.722	0.242	0.344	0.646
ISA2	0.528	0.446	0.475	0.763	0.245	0.467	0.400
ISA3	0.487	0.410	0.405	0.769	0.389	0.369	0.355
ISA4	0.528	0.491	0.511	0.786	0.445	0.427	0.354
NC3	0.407	0.416	0.438	0.422	1.000	0.413	0.252
OC1	0.589	0.603	0.523	0.458	0.340	0.761	0.335
OC2	0.617	0.563	0.573	0.427	0.357	0.820	0.302
OC6	0.563	0.592	0.527	0.373	0.290	0.814	0.260
SET2	0.361	0.353	0.365	0.601	0.267	0.342	0.888
SET3	0.284	0.332	0.288	0.609	0.202	0.289	0.875
SET4	0.346	0.330	0.290	0.651	0.239	0.341	0.901
SET1	0.333	0.286	0.320	0.594	0.175	0.342	0.853
	EA	ER	ESB	ISA	NC	OC	SET

3.4.2 Reliability

The purpose of a reliability test is to determine whether the measures are internally consistent. The dependability test can be done in two ways. First, there's Cronbach's Alpha, which has to be better than 0.6. Second, there's Composite Reliability, which requires a number larger than 0.7. Cronbach's Alpha and Composite Reliability values for each variable are dependable, according to the findings (see Table 6 and 7).

Table 6. Cronbach's Alpha Data Result

Contruct	Cronbach's Alpha	Result
Employee Accountability	0.694	Reliable
Employee Relationship	0.771	Reliable
Employee Security Behavior	0.755	Reliable
Information Security Awareness	0.764	Reliable
National Culture	1.000	Reliable
Organizational Culture	0.716	Reliable
Security Education & Training	0.902	Reliable

Table 7. Composite Reliability Data Result

Contruct	Cronbach's Alpha	Result
Employee Accountability	0.830	Reliable
Employee Relationship	0.853	Reliable
Employee Security Behavior	0.859	Reliable
Information Security Awareness	0.846	Reliable
National Culture	1.000	Reliable
Organizational Culture	0.841	Reliable
Security Education & Training	0.932	Reliable

4. RESULT AND DISCUSSION

4.1 Result

After analyzing the data, in Figure 2 and Table 8, from 9 hypotheses submitted, eight hypotheses were accepted and one hypotheses was rejected. The first hypothesis claims that employee security behavior is influenced by security education & training. The first hypothesis has a P-Value of 0.714, which indicates >0.05 and a β value of -0.017, based on the findings of the statistical analysis test. As a result of which the hypothesis H0 is accepted and the hypothesis Ha is rejected (H1 is rejected).

The second hypothesis claims that Information Security Awareness is influenced by security education & training. The second hypothesis has a P-Value of 0.000, which indicates <0.05 and a β value of 0.698, based on the findings of the statistical analysis test. As a result of which the hypothesis H0 is rejected and the hypothesis Ha is accepted (H2 is accepted).

The third hypothesis claims that Employee Relationship is influenced by security education & training. The third hypothesis has a P-Value of 0.000, which indicates <0.05 and a β value of 0.370, based on the findings of the statistical analysis test. As a result of which the hypothesis H0 is rejected and the hypothesis Ha is accepted (H3 is accepted).

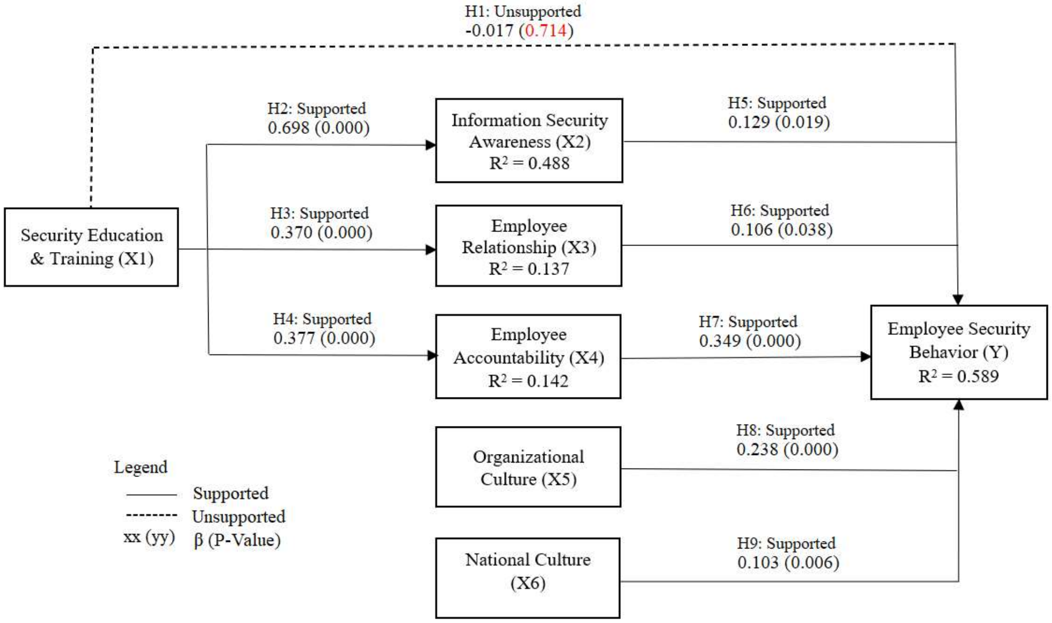

Figure 2: Result Model

Table 8. Hypthotheses Result

Variable Relation	β	P-Value	Result
Security Education & Training -> Employee Security Behavior	-0.017	0.714	Not Supported
Security Education & Training -> Information Security Awareness	0.698	0.000	Supported
Security Education & Training -> Employee Relationship	0.370	0.000	Supported
Security Education & Training -> Employee Accountability	0.377	0.000	Supported
Information Security Awareness -> Employee Security Behavior	0.129	0.019	Supported
Employee Relationship -> Employee Security Behavior	0.106	0.038	Supported
Employee Accountability -> Employee Security Behavior	0.349	0.000	Supported
Organizational Culture -> Employee Security Behavior	0.238	0.000	Supported
National Culture -> Employee Security Behavior	0.103	0.006	Supported

Table 9. Indirect Effect

Variable Relation	β	P-Value
Security Education & Training -> Employee Security Behavior	0.261	0.000

The fourth hypothesis claims that Employee Accountability is influenced by security education & training. The fourth hypothesis has a P-Value of 0.000, which indicates <0.05 and a β value of 0.377, based on the findings of the statistical analysis test. As a result of which the hypothesis H0 is rejected and the hypothesis Ha is accepted (H4 is accepted).

The fifth hypothesis claims that Employee Security Behavior is influenced by Information Security Awareness. The fifth hypothesis has a P-Value of 0.019, which indicates <0.05 and a β value of 0.129, based on the findings of the statistical analysis test. As a result of which the hypothesis H0 is rejected and the hypothesis Ha is accepted (H5 is accepted).

The sixth hypothesis claims that Employee Security Behavior is influenced by Employee Relationship. The sixth hypothesis has a P-Value of 0.038, which indicates <0.05 and a β value of 0.106, based on the findings of the statistical analysis test. As a result of which the hypothesis H0 is rejected and the hypothesis Ha is accepted (H6 is accepted).

The seventh hypothesis claims that Employee Security Behavior is influenced by Employee Accountability. The seventh hypothesis has a P-Value of 0.000, which indicates <0.05 and a β value of 0.349, based on the findings of the statistical analysis test. As a result of which the hypothesis H0 is rejected and the hypothesis Ha is accepted (H7 is accepted).

The eighth hypothesis claims that Employee Security Behavior is influenced by Organizational Culture. The eighth hypothesis has a P-Value of 0.000, which indicates <0.05 and a β value of 0.238, based on the findings of the statistical analysis test. As a result of which the hypothesis H0 is rejected and the hypothesis Ha is accepted (H8 is accepted).

The ninth hypothesis claims that Employee Security Behavior is influenced by National Culture. The ninth hypothesis has a P-Value of 0.006, which indicates <0.05 and a β value of 0.103, based on the findings of the statistical analysis test. As a result of which the hypothesis H0 is rejected and the hypothesis Ha is accepted (H9 is accepted).

In Table 9 can be seen that the exogenous variable of Security Education & Training has a significant influence on the endogenous variable of Employee Security Behavior with a P-Value of 0.000, which means < 0.05 and a β value of 0.261.

4.2 Discussion

4.2.1 Theoretical Implications

Security education & training has no substantial effect on employee security behavior, according to the findings of the study. This finding is consistent with Yaokumah et al. [4]. Then it was discovered that security education & training has a considerable impact on information security awareness, which is consistent with Connolly et al. [23].

Security education & training has a significant effect on employee relationships. This finding is in accordance with the research of Yaokumah et al. [4], but in this study the value is greater, namely 0.370, compared to research from Yaokumah et al. [4] which is 0.219. Then the Security education & training also has a significant effect on employee accountability with a value of 0.377, where this finding is in accordance with research from Yaokumah et al. [4] which has a greater value, which is 0.457.

It was also found that information security awareness has a significant effect on employee security behavior, where this finding is in accordance with research from Connolly et al. [23]. Another factor that has a significant effect on employee security behavior is employee relationships. This finding is in accordance with the research of Yaokumah et al. [4], but has a smaller effect, namely 0.106, compared to research from Yaokumah et al. [4], namely 0.269. Then, employee accountability also has a significant effect on employee security behavior, where this finding is in accordance with research from Yaokumah et al. [4], but has a greater effect, namely 0.349, compared to research from Yaokumah et al. [4], namely 0.215.

From the results of the analysis, it was also found that organizational culture has a significant effect on employee security behavior, where this finding is in accordance with research from Connolly et al. [25]. This finding is also the same for the national culture with research from Connolly et al. [25].

4.2.2 Practical Implications

The results of data analysis in this study revealed that security education & training has no significant effect on employee security behavior. However, from the results of the questionnaire in the descriptive analytic, it was also found that on average the respondents agreed with the good quality of the information system security training that had been provided, which meant that the quality of the information system security training provided by the company was currently good and needed to be maintained.

Meanwhile, security education & training has a significant effect on the mediators (information security awareness, employee relationship and employee accountability). With this finding, the companies must pay attention to the availability of security education & training programs and the quality of the material provided to employees, especially non-IT employees, so they can be more aware and more responsible for the importance of maintaining the security of company information system and know what they should do.

It was also found that information security awareness has a significant effect on employee security behavior. With this results, the companies must pay attention to the level of employee information security awareness, namely by periodically measuring the level of employee information security awareness using existing measurement methods, such as Multiple Criteria Decision Analysis (MCDA) [27], so that the level of employee information security awareness can be managed properly.

Another factor that has a significant effect on employee security behavior is employee relationships. With this result, the companies must build a good relationships with their employees, both in communication, guidance and discipline, so it could increase employee satisfaction at work and a high commitment to maintaining company business secrets.

Then employee accountability also has a significant effect on employee security behavior. Therefore, the companies must be able to build accountability in each employees by presenting a responsible leader who enforces the rules well and firmly.

From the results of the analysis, it was also found that organizational culture has a significant effect on employee security behavior. With this result, the companies must create a good organizational culture in several ways, including providing clear SOPs and positions to employees, providing fair and professional career opportunities, setting short-term and long-term targets, encouraging employees to continue to do self-improvement. Thus, a positive organizational culture will be created which can later influence the way they behave, including behavior in using the company's information system.

National culture was also considered to have a significant effect on employee security behavior. Based on these findings, the companies must pay attention to the characteristics of each of their employees, whether typically collectivism or individualism, where these two characteristics can have an impact on a person's behavior in the organization.

5. CONCLUSION

Security education and training had no direct or meaningful influence on increasing employee security behavior in Jabodetabek, according to this study. The security education & training influences the mediators (information security awareness, employee relationship and employee accountability), and the mediators influences employee behavior in using the company's information system. The most influential variable is employee accountability. Organizational culture and national also culture influence employee behavior in using company information systems.

This paper contributed to the companies in Jakarta greater area in making the right strategy to anticipate threats to the security of their information systems by employees, also for Indonesian government in making or improving regulations related to the confidentiality of company information, and also for IT consultants in providing the best solutions for their clients in dealing with internal threats.

REFERENCES

[1] BSSN (2020) “Laporan hasil monitoring Keamanan Siber Tahun 2020”, 56 – 57.

[2] Abawajy, J. (2014), “User preference of cyber security awareness delivery methods” Behaviour & Information Technology, 33(3), 237–248. doi:10.1080/0144929X.2012.708787

[3] Marett, K. (2015),"Checking the manipulation checks in information security research", Information & Computer Security, Vol. 23 Iss 1 pp. 20 – 30.

[4] Crossler, R.E., Allen, Johnston, Lowry, P.B., Hu, Q., Warkentin, M., Baskervil, R. (2013), “Future directions for behavioral information security research”, Computer & Security 32, 90 – 101.

[5] 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.

[6] Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012), “Managing employee compliance with information security policies: The critical role of top management and organizational culture”, *Decision Sciences*, *43*(4), 615-660.

[7] Islami, D. C., IH, K. B., & Candiwan, C. (2016), ” Kesadaran Keamanan Informasi pada Pegawai Bank x di Bandung Indonesia”, INKOM Journal, 10(1), 19–26.

[8] Xu, Z., & Guo, K. (2019), “It ain’t my business: A coping perspective on employee effortful security behavior”, *Journal of Enterprise Information Management*.

[9] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010), “Quality and fairness of an information security policy as antecedents of employees’ security engagement in the workplace: An empirical investigation”, 43rd Hawaii International Conference on System Sciences, 1–7.

[10] Straub Jr, D. W. (1990), “Effective IS security: An empirical study”, Information Systems Research, 1(3), 255–276.

[11] Tsui, A. S., Zhang, Z.-X., Wang, H., Xin, K. R., & Wu, J. B. (2006), “Unpacking the relationship between CEO leadership behavior and organizational culture”, The Leadership Quarterly, 17(2), 113–137.

[12] Keyton, J. (2014), "Communication, organizational culture, and organizational climate", The Oxford Handbook of Organizational Climate and Culture, 118–135.

[13] Smircich, L. (2017), "Concepts of culture and organizational analysis", The Anthropology of Organisations, 255–274.

[14] Kilmann, R., H. (1985), "Managing your organization's culture", The Nonprofit World Report, 3(2), 12–15.

[15] Ali, M., & Brooks, L. (2008), "Culture and IS: National cultural dimensions within IS discipline".

[16] Hofstede, G., Neuijen, B., Ohayv, D., D., & Sanders, G. (1990), "Measuring organizational cultures: A qualitative and quantitative study across twenty cases", Administrative Science Quarterly, 286–316.

[17] Kaspersky, E., & Furnell, S. (2014), "A security education Q&A", Information Management & Computer Security.

[18] McCrohan, K. F., Engel, K., & Harvey, J. W. (2010), "Influence of awareness and training on cyber security" Journal of Internet Commerce, 9(1), 23–41. doi:10.1080/15332861.2010.487415

[19] Vance, A., Lowry, P. B., & Eggett, D. (2013), "Using accountability to reduce access policy violations in information systems", Journal of Management Information Systems, 29(4), 263–290. doi:10.2753/MIS0742- 1222290410

[20] Zaman, U., & Saif, M. I. (2016), "Perceived accountability and conflict management styles as predictors of job performance of public officials in Pakistan", Gomal University Journal of Research, 32(2), 24–35.

[21] Gennard, J., & Judge, G. (2005), "Employee relations"' CIPD Publishing.

[22] Trček, D., Trobec, R., Pavešić, N., & Tasič, J. F. (2007), "Information systems security and human behaviour", Behaviour & Information Technology, 26(2), 113–118.

[23] Connolly, L. Y., Lang, M., & Tygar, D. J. (2018), "Employee security behaviour: the importance of education and policies in organisational settings", In Advances in Information Systems Development (pp. 79–96). Springer.

[24] Sivalogathasan, V., & Hashim, A. (2013), "CHANGES IN EMPLOYER-EMPLOYEE RELATIONSHIP: IMPACT OF PERCEIVED ORGANIZATIONAL SUPPORT ON SOCIAL EXCHANGE OF THE OUTSOURCING INDUSTRY IN SRI LANKA", Skyline Business Journal, 9(1).

[25] Connolly, L., Lang, M., & Tygar, J. D. (2015), "Investigation of employee security behaviour: A grounded theory approach", IFIP International Information Security and Privacy Conference, 283–296.

[26] Ringle, C. M., Wende, S., & Becker, J.-M. (2015), "SmartPLS 3. Boenningstedt: SmartPLS GmbH", Retrieved from http://www.smartpls.com

[27] Amin, M. (2014), "Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (MCDA)", Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika Vol, 5(1).