Journal of Theoretical and Applied Information Technology
31st December 2022. Vol.100. No 24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ANALYSIS OF THE EFFECT OF ORGANIZATIONAL CULTURE, SECURITY COUNTERMEASURES, AND NATIONAL CULTURE ON USER SECURITY BEHAVIOUR IN PT NUSA NETWORK PRAKARSA

[1] JAROT S. SUROSO, [2] HAFIZH FIISABILILLAH, [3] MUHAMMAD FADHIL A.S.

[1,2,3] Information Systems Management Department, Binus Graduate Program, Bina Nusantara University, Jakarta, Indonesia 11480, Indonesia

E-mail: [1] jsembodo@binus.edu, [2] hafizh@binus.ac.id, [3] muhammad.suroso@binus.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% of external attacks. Currently, the PT Nusa Network Prakarsa organization which is engaged in IT solutions found that there were several malicious anomalies based on daily, weekly, and monthly firewall reports. This study aims to examine the influence of Organizational Culture, Security Countermeasures, and National Culture on User Security Behavior at PT Nusa Network Prakarsa. The sample of this research is employees who work at PT Nusa Network Prakarsa. The sample was carried out using the Likert Scale method, data collection was carried out by questionnaires distributed directly to employees as many as 160 respondents. Statistical method using Linear Regression Analysis, with statistical test hypothesis testing

Keywords: *Internal threat, Organisational Culture, Security Countermeasures, National Culture, dan User Security Behaviour*

1. INTRODUCTION

Information is a value, and more and more organizations are realizing that information security risks can have a negative impact on the viability of business processes and public image, it can also cause financial loss, affect relationships, and satisfaction with clients and partners. “Information security is the protection of information and its important elements. Confidentiality, integrity, and availability of information are the three main characteristics of information security. Confidentiality ensures that information is only accessed by those with special privileges” [1]

Internal threats have been a hot topic in information security for several years, but the statistics on this topic are not very interesting. According to an Insider Threat Reports survey in 2018, 51% of users are more concerned about internal carelessness and negligence than 47% of external attacks. [2]

Also as many as 56% of users prefer regular employees who have the potential to become internal threats. Moreover, as many as 67% of users see the threat of attempted phishing attacks on employees as a potential opening for internal threats to occur.

Currently, the PT Nusa Network Prakarsa organization which is engaged in IT solutions found that there were several malicious anomalies based on daily, weekly, and monthly firewall reports. [2]

Based on PT Nusa Network's monthly firewall security system report, it can be seen that employee activities are monitored by an anomaly system which shows that many viruses have been caught by the system due to the negligence of PT Nusa Network's employees.

Also, monitored by an anomaly system which shows that many sites visited are potentially dangerous, inviting malicious malware as well as due to the lack of knowledge of PT Nusa Network employees.

Moreover, it is monitored by a graphical system which shows that many domains visited are a high threat according to the system.

Today, organizations are totally dependent on information systems to improve productivity performance, resulting in competitive advantage and achieving strategic goals. However, users of

information systems are vulnerable to both intentional and unintentional security risks. [3] stated that users tend to be the main contributing factor in many information security breaches. Thus, an increasing amount of attention is being paid to the security side of human information. According to [4], employee security behavior is the main cause of many data breaches in organizations. Information security breaches often occur in organizations due to employee ignorance or careless behavior. For example, employee negligence or malicious accounts 78% of data breaches in organizations, as a result, organizational leaders are looking for solutions to influence positive changes in employee behavior towards the security of information resources.

According to the important aspect in managing employee security behavior in the organization is through security education, training, and awareness or can be called security countermeasures. Information security education is an attempt to make employees aware of the security environment, policies, and security of the organization [5] A growing body of evidence suggests that information security can be used to improve employee information security behavior. The main reason organizations provide Education, training, and awareness programs to reduce unwanted employee safety behavior towards the organization's information resources. Through the use of effective training techniques, employees can be educated about how to make a decision secure information security [3]

However, a comprehensive literature review conducted for this study revealed that a number of areas of research require further investigation. Some researchers suggest that the deterrent factor may vary under the impact of other aspects. The literature review conducted reveals a limited number of studies investigating the effect of deterrent factors in combination with cultural aspects. In addition, cross-cultural studies have been very rare in previous behavioral research. Although research [3] shows that national culture influences organizational behavior,[1] reports that there is a general lack of studies examining the effects of organizational culture on employee security behavior and existing studies fail to link organizational culture with security behavior. employee

2. LITERATURE REVIEW

2.1 Information Security Within The Company

Statistics show that most of the economic activity is contributed by companies and the growth of the internet and dependence on information technology has increased various threats to information security and therefore can have a negative impact on business [5]

Management of information security within the enterprise and the gap between different sizes of organizations is a direct result of the available money, technical resources that companies can invest in protecting against internal threats. The main obstacles for the company are:

1 .Staffs with limited security experience

2. Lack of finance to hire external consultants or provide employee training.

3. Lack of understanding of risk

4. Inability to focus on security due to the need to focus on other business needs.

[4] focuses on the information security culture within the company, and the main findings are: companies have less security knowledge and understanding about the importance of information security in business, minimal reports on security incidents

[1] agree that company management does not provide the necessary time and budget for information security. According to his research, the majority of companies do not have information security policies. This finding also proves the conclusion of other researchers that companies have limited human resources for security tasks and management's lack of understanding about the importance of information security in organizations, noting that the company's information security budget is usually very tight. However, not only is the information security budget an important distinction for companies, it is also the lack of awareness about information security.

The importance of information security awareness is a serious issue that should be handled with care, but researchers have different views about what constitutes an internal threat and why and how insiders negatively affect information security. Some of them focus on internal threats with malicious intent, for example stating that the majority (88%) of people in planning their Actions. According to [6], information security threats can be categorized into three groups based on motivation:

Examples of employee security behavior include how staff members handle their passwords, how they handle organizational data, and how they use network resources. This behavior can pose an information security threat. This study does not focus on a specific type of behavior but at the same

time aims to distinguish between positive and negative behavior because the factors that influence these actions can vary.

2.2 User Security Behaviour.

Employee security behavior is defined as employee behavior in using the organization's information systems (including hardware, software, and network systems). And such behavior may have security implications. Examples of employee security behavior include how staff members handle their passwords, how they handle organizational data, and how they use network resources. This behavior may create or reduce an information security threat. This study does not focus on a particular type of behavior but at the same time aims to distinguish between positive and negative behavior because the factors that influence the Action may be different [7]

Furthermore, behavior of interest includes compliant behavior (i.e. complying with organizational policies, procedures and norms in relation to information security) and non-conforming behavior, i.e. intentional but harmless behavior of employees that may be carried out and result in non-compliance with organizational policies, procedures and norms. in relation to information security [8]

According to [1] there are two groups of factors that influence employee behavior. The first group consists of users' knowledge of what the organization expects of them, the second group consists of factors that influence employees' willingness to limit themselves to appropriate behavior.

[1] also states that bad or unacceptable employee behavior is one of the main causes of security incidents in organizations and not only intentional security attacks, but also user security errors, carelessness and negligence are a serious threat to information security. [9] also agrees with Leach's idea that accidents are often the result of our subconscious activities. So in this thesis every incident caused by an internal person and has a negative impact on information security is considered an internal threat.

2.3 Organizational Culture

According to [10] , organizational culture is described as a separate and hidden force that controls behavior and attitudes in organizations. In addition, culture as a guide perceptions, thoughts, feelings, and acceptable behavior among group members. Finally, the researcher emphasizes the importance of organizational culture as a force that can lead a company to success or weaken its vitality because organizational culture directly affects the behavior of employees in an organization.

This is supported by [4] that organizational culture influences behavior, and as a separate and hidden force that controls behavior and attitudes in organizations. Furthermore, [11] describes culture as a set of assumptions tacitly guiding perceptions, thoughts, feelings, and acceptable behavior among group members. Finally, [12] emphasizes the link between organizational culture and behavior, this subject area has received little attention in behavioral infosec research, a literature review conducted for this research revealed a lack of studies of organizational culture in the security context.

[4] present an expanded deterrence theory and report that security precautions such as security policies, awareness programs, and computer monitoring affect the perceived severity of formal sanctions, leading to reduced intentions to abuse information systems. Furthermore, the researchers show that preventive-based precautions, including information security policies, security education and training awareness programs, and security systems, directly influence security behavior in organizations.

2.4 National Culture

According to [5] , National culture influences the behavior of employees especially organizations. According to researchers, organizations are bound by national culture and underline cross-national differences in the functioning of the people in it. National culture is the core values, norms, and practices in society that shape the behavior of individuals in society. Various academic works also show that national culture influences organizational behavior.

[13] argues that Irish organizations typically implement reciprocal adjustment mechanisms to coordinate activities and establish adhocracy structures, of which support staff are an important part. Mutual adjustment achieves coordination of work by a simple process of informal communication and control of work rests with the actors. On the other hand, the United States takes a fragmented form, based on standardization where usually, American companies standardize by setting specific goals and outcomes. Previous studies have shown that employees tend to evade security rules when under pressure to meet deadlines. Therefore, the factors that force employees to violate security

rules may differ in the United States and Ireland due to different organizational structures.

2.4 SEM-PLS

According to [14] , Partial Least Square (PLS) is a structural equation model orientation that is used to test theories or to develop theories (prediction purposes). PLS is an alternative approach that shifts from a covariance-based Structural Equation Modeling (SEM) approach (measuring the magnitude of the relationship between two variables) to a variance-based (measure of correlation between the same two random variables). PLS is often applied for three reasons, namely data attribution, sample size, and the use of formative indicators. As stated by [14] this method is a very strong method, because it is not based on many assumptions, the data does not have to be normally distributed multivariate (indicators with a categorical scale to the ratio can be used in the same model) and for sample materials do not have to be A large sample with a minimum sample of 30-50 can be applied and is feasible to be used as a research sample. Meanwhile, according to [15]PLS is a "powerful" analytical method because it can be applied to all data scales, does not require many assumptions and the sample size does not have to be large.

Based on the theories above, this study conducts research on where the variables used are Organizational Culture, Security Countermeasures, and National Culture that affect Employee Security Behavior:

According to [16] The following are examples of work culture models based on studies conducted on work culture that have shown :

1. Authoritarian Work Culture
2. Individual Work Culture
3. Collectivity Work Culture

[17] argue that typically Irish organizations implement reciprocal adjustment mechanisms to coordinate activities and establish adhocracy structures, of which support staff is an important part. Mutual adjustment achieves coordination of work by a simple process of informal communication and control of work rests with the actors. On the other hand, the United States takes a fragmented form, based on standardization where usually, [18] American companies standardize by setting specific goals and outcomes. Previous studies have shown that employees tend to evade security rules when under pressure to meet deadlines. Therefore, the factors that force employees to violate security rules may differ in the United States and Ireland due to different organizational structures.

According to [19] The following are examples of work culture models based on studies conducted on work culture that have shown certain models, namely authoritarian culture, bureaucratic culture, task culture, individualistic culture, bargaining culture and collectivist culture, namely :

1. Authoritarian Work Culture

This type of work culture focuses on 'command and control'. Power and authority in an organization is usually centered on the leader. Employees will be expected to show high loyalty to the leader. Directions and regulations are sent from the top to the bottom of the organization. This form of culture is often effectively practiced in small-sized organizations such as family business establishments, small companies and simple firms.

Thus, a close personal relationship with the superior is an important factor in smooth work and promotion.

2. Individualistic Work Culture

In this work culture, certain individuals become the main focus. There are universities that rely on top professors to attract students and earn scholarships. Likewise, consulting or guaman firms usually rely entirely on certain popular individuals (consultants or lawyers) to attract customers. In this culture, a small number of workers are the backbone of the success of the company because they have reputation, credibility, intelligence and skills. The ability to get customers often causes them to be less bound to rules and procedures.

3. Collective Work Culture

It is said that one of the keys to the success of Japanese culture is their ability to use the ideas and reserves of subordinate workers. This is because workers are 'owners of the work process' and they know more about systems and procedures for carrying out work than other people. With that workers are given the opportunity to express suggestions and creativity to improve work processes, systems and procedures.

2.5 Security Countermeasures

With the increasing incidence of computer abuse by employees, organizations are looking for better ways to prevent it, according to [4] organizations can improve employee compliance with information security rules by implementing preventive mechanisms, including technical controls, security policies. information (security policy), security

education (education), training (training) and awareness programs (security awareness). Prevention theory is one of the most widely applied theories in information system security. Classical deterrence theory suggests that individuals weigh the costs and benefits before committing a crime. If someone believes that the risk of being caught is high and penalties will be applied if caught.

Based on the theories above, this study conducts research on where the variables used are Organizational Culture, Security Countermeasures, and National Culture that affect Employee Security Behavior:

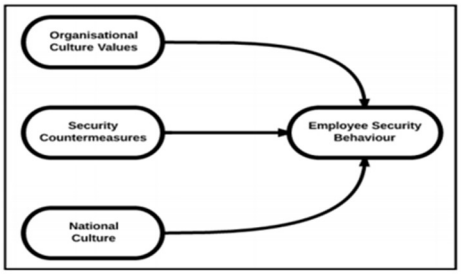

Figure 1 : Research Methodology : [4]

3. RESEARCH METHODOLOGY

The purpose of this study is to determine whether organizational culture, national culture, and security countermeasure factors affect employee behavior towards information security systems. After conducting a literature review on related topics, it was found that there are still few studies in Indonesia that discuss employee security behavior towards information security systems. Therefore, the author uses several studies that are related to the topic and because this topic is still rarely studied, the author uses a modified model from several previous research models to help determine how much impact employee behavior has on information system security

Based on survey data shown by [2] shows that as many as 51% of users are more concerned with carelessness and negligence from internally than 47% of attacks from outside, it is concluded that there are factors that cause this concern to be very high compared to with external factors, the topic that arises is what factors cause internal data security information to be very vulnerable.

From the results of a brief survey that has been carried out, it also indicates that as many as 56% of regular employees have the potential to become internal threats. Therefore, the authors are interested in examining what factors can influence employee behavior that can threaten the company's information security.

Moreover, the Antivirus and Web filter system reports on PT Nusa Network Prakarsa's security devices also show anomalies as well as internal carelessness and negligence of employees

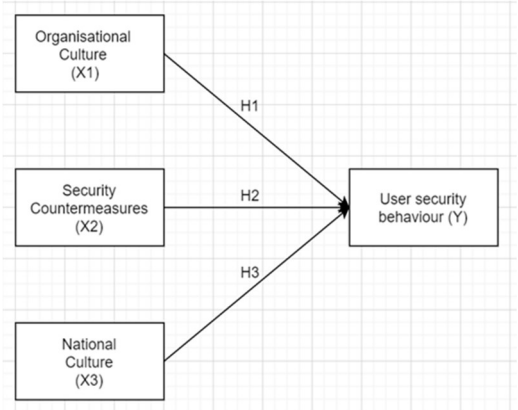

Figure 2. Research Methodology

H1: Variable organizational culture affects user security behavior variables.
H2: Variable security countermeasures affect the variable user security behavior.
H3: Variable national culture has an effect on variable user security behavior.

Table 1. Variable And Indicator

No	Variable	Simbol	Indikator	Source
1	*Organisational Culture*	OC1	The drive to innovate	Winfred Yaokumah, Daniel Okyere Walker, and Peace Kumah (2019)
		OC2	Employees work carefully	Winfred Yaokumah, Daniel Okyere Walker, and Peace

				Kumah (2019)
		OC3	Demanded more berkualitas	Winfred Yaokumah, Daniel Okyere Walker, and Peace Kumah (2019)
		OC4	Teamwork	Winfred Yaokumah, Daniel Okyere Walker, and Peace Kumah (2019)
		OC5	Compete with each other	Winfred Yaokumah, Daniel Okyere Walker, and Peace Kumah (2019)

No	Variable	Simbol	Indikator	Source
2	*Security Counter measures*	SC1	Password is a password to enter a system	Winfred Yaokumah, Daniel Okyere Walker, and Peace Kumah (2019)
		SC2	Phishing can cause both financial and non-financial losses	Winfred Yaokumah, Daniel Okyere Walker, and Peace Kumah (2019)
		SC3	The use of any information must be done with the approval of the company	Winfred Yaokumah, Daniel Okyere Walker, and Peace Kumah (2019
		SC4	Education about information security responsibilities.	Winfred Yaokumah, Daniel Okyere Walker, and Peace Kumah (2019)
		SC5	All employees are regularly tested for their knowledge of safety procedures.	Winfred Yaokumah, Daniel Okyere Walker, and Peace Kumah (2019)

No	Variable	simbol	Indikator	Source
3	National Culture	NC1	Individualisme	Lena Connolly, Michael Lang, and J.D Tygar (2015)
		NC2	Kolektivisme	Lena Connolly, Michael Lang, and J.D Tygar

				(2015)
		NC3	Uncertainty and Ambiguity	Lena Connolly, Michael Lang, and J.D Tygar (2015)
		NC4	Obedience	Lena Connolly, Michael Lang, and J.D Tygar (2015)

Below are the data collection methods used during the study:
1. Literature review
In this method, the author collects data by reading and analyzing books, journals about previous similar research, or articles to serve as a basis or research.

2. Questionnaire Distribution
To test the hypothesis of research on factors that influence employee behavior, data is needed, the data can be obtained through the distribution of questionnaires using Google form tools which will be distributed later. The use of the technique in sampling is simple random sampling by dividing a group (strata) and taking random samples. The questionnaire will be arranged based on a Likert scale using 5 internals. From the data, the number of workers at the Nusa Network company is 200 people and will be used as a population reference for this study. The sample needed to represent the population is calculated using the formula from Slovin, namely:

Information:
n = sample size
N = population size
e = error rate
n = 200 = (1+100*0.05*0.05)
n = 160 Respondents

Table 2. Likert Scale

Category Scale	Scale Point
Very Not Agree	1
Not Agree	2
Netral	3
Agree	4
Very Agree	5

From the data, the number of workers at the Nusa Network company is 200 people and will be used as a population reference for this study. The sample needed to represent the population is calculated using the formula from Slovin, namely:

$$n = \frac{N}{Ne^2+1}$$

Information:
n = sample size
N = population size
e = error rate
n = 200 = (1+100*0.05*0.05)
n = 160 Respondents

Y = 10 + 11X1 + 12X2 + 13X3 +∈1.... 1
Based on the structural model above, the regression equation of the model is as follows:
Hypothesis 1 (H1):
H0 : 11 = 0, then Organizational Culture has no significant effect on Employee Security Behavior
H0 : 11 0, Then Organizational Culture has a significant influence on Employee Security Behaviour
Hypothesis 2 (H2):
H0 : 12 = 0, then Security Countermeasures does not have a significant effect on Employee Security Behaviour
H0 : 12 0, then Security Countermeasures have a significant effect on Employee Security Behaviour
Hypothesis 3 (H3):
H0 : 13 = 0, then National Culture has no significant effect on Employee Security Behaviour
H0 : 13 0, then National Culture has a significant influence on Employee Security Behaviour

In this study data collection using a questionnaire, because it is necessary to have a measuring instrument to determine the validity and reliability. There are two important requirements that apply to a questionnaire, namely the necessity of a questionnaire to be valid and reliable. Validity test is a form of testing the quality of primary data, with the aim of measuring the validity of a question in research. The instrument is said to be valid, meaning that the instrument can be used to measure what should be measured.

The validity test consists of 2 types, namely the convergent validity test which can be done in

several ways including by looking at the loading factor value on each indicator with a value that must be > 0.7 or through the Average Variance Extracted (AVE) value on each variable with a value of > 0.7. The second test is the discriminant validity test which can be done in several ways including the Fornell Larcker Criterion test and the Cross Loading test.

Reliability test is a tool to measure a questionnaire which is an indicator of a variable or construct. A questionnaire is said to be reliable or reliable if a person's answer to a question is consistent or stable over time.

The reliability test can be done by calculating the Cronbach's Alpha value provided that if the value is > 0.7 then it is reliable (Sarstedt et al., 2020). In addition, the reliability test can also be done by looking at the Composite Reliability value provided that if the value is > 0.7 then it is reliable.

Table 3. Research Object

No	Unit	Business Process
1	Product	Introducing products to customers
2	Sales	Finding and maintaining relationships with customers
3	Finance	Manage financial planning
4	IT	Perform device installation and preventive maintenance of the device
5	HR	Managing human resources, Managing employee assignments, managing employee attendance, and Managing employee performance administration

PT Nusa Network is a company in Indonesia that provides network and security solution services and solutions complete with the Vision and Mission, namely:
a. Vision : “To be a trusted digital transformation solution partner who is responsible for managing and developing the life cycle of customer technology”
b. Mission: "Providing maximum service with a high commitment to increasing professionalism"
Currently, Nusa Network has its main business in each Stakeholder related to the use of related Information Technology

Currently, PT Nusa Network has approximately 200 employees, with an organizational structure such as:

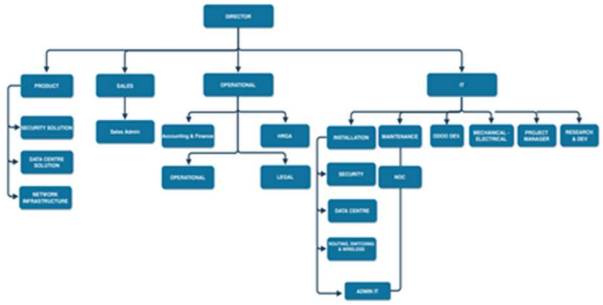

Figure 3: Organization Structure

4. RESULT AND DISCUSSION

An indicator must represent 1 latent and underlying variable the latent variable. For this reason, a convergent validity test is needed. Test Convergent validity can be done in several ways, including: by looking at the value of the loading factor, namely the value generated by each indicator to measure the variable or by looking at the Average Variance Extracted (AVE) value. This value describes sufficient convergent validity which means that one latent variables are able to explain more than half the variance of the indicators are in average.

Table 4 Convergent Validity Test Result Basedon Loading Fact Values

Indikator Variabel	Outer Loading	Limit Value	Result
Organisational Culture			
OC1	0.913	> 0.7	Valid
OC2	0.922	> 0.7	Valid
OC3	0.933	> 0.7	Valid
OC4	0.935	> 0.7	Valid
OC5	0.939	> 0.7	Valid

Security Countermeasures			
SC1	0.933	> 0.7	Valid
SC2	0.946	> 0.7	Valid
SC3	0.931	> 0.7	Valid
SC4	0.921	> 0.7	Valid
SC5	0.937	> 0.7	Valid
National Culture			
NC1	0.936	> 0.7	Valid
NC2	0.942	> 0.7	Valid
NC3	0.936	> 0.7	Valid
NC4	0.929	> 0.7	Valid
User Security Behaviour			
USB1	0.938	> 0.7	Valid
USB2	0.935	> 0.7	Valid
USB3	0.939	> 0.7	Valid
USB4	0.939	> 0.7	Valid
USB5	0.935	> 0.7	Valid

Table 5. Convergent Validity Test Result Based on AVE

Variable	Average Variance Extracted (AVE)	Minimum Value	Result
Organisational Culture	0.875	> 0.7	Valid
Security Countermeasures	0.862	> 0.7	Valid
National Culture	0.871	> 0.7	Valid
User Security Behaviour	0.879	> 0.7	Valid

From Tables it is found that all indicator in this test has a valid value on each of the parameters that used.

In the reliability test there are several ways, namely by analyzing Cronbach's Alpha and Composite Reliability. The results of the reliability test This research can be seen in Table 6

Table 6: Reliability Test Result Based on Cronbach's Alpha

Variable	Cronbach Alpha	Limit Value	Result
Organisational Culture	0.960	>0.7	Reliable
Security Countermeasure	0.963	>0.7	Reliable
National Culture	0.953	>0.7	Reliable
User Security Behaviour	0.965	>0.7	Reliable

Table 7 Reliability Test Result Based on Composite Reliability

Variable	Composite Reliability	Limit Value	Result
Organisational Culture	0.969	>0.7	Reliable
Security Countermeasure	0.971	>0.7	Reliable
National Culture	0.966	>0.7	Reliable
User Security Behaviour	0.973	>0.7	Reliable

From Tables 5 it is found that all variables in this test the value is reliable on each parameter used.

Hypothesis analysis was carried out through the bootstrapping method. Level The significance used is 5%, meaning that the relationship between variables said to be significant if the p-values <0.05. Table 4.19 below are the results of the p values obtained from the test and the results of the research model .

Table 8: Result P-Values Evaluation

Variable Relationship	β	P-Values	Result
Organisational Culture -> User Security Behaviour	0.493	0.622	No Significant Effect
Security Countermeasures -> User Security Behaviour	3.979	0.000	Significant Effect
National Culture -> User Security Behaviour	4.774	0.000	Significant Effect

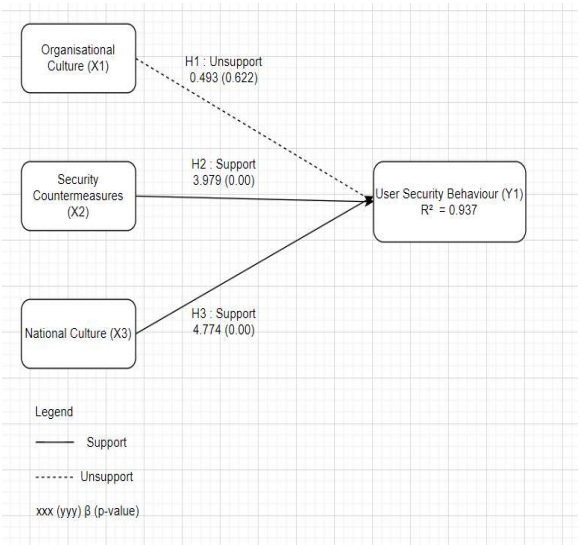

Figure 3 : Result Research Model

a. Hypothesis Analysis 1 (H1)

In the results of hypothesis testing 1 (H1), namely the influence of the Organisational Culture variable on the User Security Behaviour, the p-value >0.05, Therefore, H1 which states that there is no significant influence between Organisational Culture variables on User Security Behaviour. This is in accordance with the author's limited interview, that Organisational Culture indeed considered to have no significant effect on User Security Behaviour.

b. Hypothesis Analysis 2 (H2)

In the results of hypothesis testing 2 (H2), namely the influence of the Security Countermeasure variable on the User Security Behaviour, the p-value <0.05, Therefore, H1 which states that there is significant influence between Security Countermeasure variables on User Security Behaviour. This is in accordance with the author's limited interview, that Security Countermeasure indeed considered to have significant effect on User Security Behaviour.

c. Hypothesis Analysis (H3)

In the results of hypothesis testing 3 (H3), namely the influence of the National Culture variable on the User Security Behaviour, the p-value <0.05, Therefore, H1 which states that there is significant influence between National Culture variables on User Security Behaviour. This is in accordance with the author's limited interview, that National Culture indeed considered to have significant effect on User Security Behaviour.

After carrying out statistical analysis on each hypothesis raised in this study, it can be seen that the National Culture variable is the variable that most influences User Security Behavior because it has the largest value of 4.774, meaning that every increase in the value of the National Culture variable by 1 unit will increase the value of the User Security Behavior variable is 4.774 with the assumption that other variables are fixed.

After doing Based on the results of the analysis, the variables of Security Countermeasures and National Culture have a significant effect on User Security Behavior. This result is in line with previous research (Yakoumah, 2019) but in this study Security Countermeasure has a greater influence than previous studies (0.219) and National Culture is also higher than previous

studies (0.269) . Then in previous research (Chengli, 2013) also confirmed that Security Countermeasure and National Culture had the same significant effect on User Security Behavior with an effect of (0.311) and (0.046), smaller than this study. Organizational Culture is considered not to have a significant effect on User Security Behavior. These results confirm previous research (Yakoumah, 2019), that this variable has no significant effect on User Security Behavior.

The results of the study which explain that Security Countermeasures are considered to have an effect on User Security Behavior, the PT Nusa Network Prakarsa company should pay more attention to the handling and implementation of security awareness for staff, such as providing training or seminars on security awareness, this will cost money but this cost is not comparable with data loss or loss due to hacking. This is also so that employees have the mindset that data security is not only for the needs of the organization but also part of the work culture that needs to be preserved.

Likewise with National Culture which is considered to have a significant effect on User Security Behavior. With these results, the PT Nusa Network Prakarsa company must realize that employee behavior in Indonesia shows that employee security actions are driven by a combination of factors, including individual interests and group aspects. Also peer influence is stronger because of differences in Individualism, therefore, PT Nusa Network Prakarsa needs to focus on security and training based on national culture.

Data analysis also shows that the variable that most influences User Security Behavior is the National Culture variable. With this result, the PT Nusa Network Prakarsa company should have a stricter security policy, because sometimes due to national cultural factors, after implementing certain security, someone in a managerial position may ask to have access to something that is prohibited to access, and if a peer is a person who holds access, acceptance will occur and they will not notify anyone of this violation. rules should be there for everyone.

5. CONCLUSION

1. This study proves that the Organizational Culture variable does not affect User Security Behavior

2. This study proves that the Security Countermeasures variable affects User Security Behavior

3. This study proves that the National Culture variable influences and becomes the most influential factor on User Security Behavior.

3. So, it was found that the User Security Behavior orientation leads to a National Culture, so it is hoped that the PT Nusa Network Prakarsa Company will pay more attention to and increase stricter rules, awareness and security on employee behavior. For further research, can explain and analyze a wider scope such as comparisons within companies in Jabodetabek, or comparisons in various fields of companies. or further research, add other variables, such as Organization Size, because in this study PT Nusa Network Prakarsa is a medium size organization and can then analyze and compare companies in various Organization Sizes.

REFERENCES

[1] J. Leach, “Improving user security behaviour,” *Comput. Secur.*, vol. 22, no. 8, pp. 685–692, 2003, doi: 10.1016/S0167-4048(03)00007-5.

[2] Cybersecurity Insiders, “Insider threat 2018,” p. 41, 2018, [Online]. Available: https://crowdresearchpartners.com/wp-content/uploads/2017/07/Insider-Threat-Report-2018.pdf.

[3] W. Yaokumah, D. O. Walker, and P. Kumah, “SETA and security behavior: Mediating role of employee relations, monitoring, and accountability,” *J. Glob. Inf. Manag.*, vol. 27, no. 2, pp. 102–121, 2019, doi: 10.4018/JGIM.2019040106.

[4] L. Connolly, M. Lang, and J. D. Tygar, “Investigation of employee security behaviour: A grounded theory approach,” *IFIP Adv. Inf. Commun. Technol.*, vol. 455, pp. 283–296, 2015, doi: 10.1007/978-3-319-18467-8_19.

[5] L. Y. Connolly, M. Lang, and D. J. Tygar, *Employee security behaviour: The importance of education and policies in organisational settings*, vol. 26. Springer International Publishing, 2018.

[6] T. Schlienger and S. Teufel, “Management,” no. September 2018, 2002, doi: 10.1007/978-

0-387-3558.
[7] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, 2006, doi: 10.1016/j.cose.2006.02.008.
[8] D. Liu, X. Wang, and L. J. Camp, "Mitigating inadvertent insider threats with incentives," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5628 LNCS, no. February, pp. 1–16, 2009, doi: 10.1007/978-3-642-03549-4_1.
[9] M, "Computer Security Handbook , 4th Edition Computer Security Handbook , 4th Edition," pp. 1–16, 2002.
[10] E. Sherif, S. Furnell, and N. Clarke, "An identification of variables influencing the establishment of information security culture," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9190, no. January 2016, pp. 436–448, 2015, doi: 10.1007/978-3-319-20376-8_39.
[11] D. Bingöl, İ. Şener, and E. Çevik, "The Effect of Organizational Culture on Organizational Image and Identity: Evidence from a Pharmaceutical Company," *Procedia - Soc. Behav. Sci.*, vol. 99, pp. 222–229, 2013, doi: 10.1016/j.sbspro.2013.10.489.
[12] L. Cheng, Y. Li, W. Li, E. Holm, and Q. Zhai, "Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory," *Comput. Secur.*, vol. 39, no. PART B, pp. 447–459, 2013, doi: 10.1016/j.cose.2013.09.009.
[13] I. Journal and C. C. Management, "• Geert Hofstede , Culture ' s Consequences : Comparing Values , Behaviours , Institutions , and Organizations Across," no. April, 2016.
[14] I. Ghozali, "Partial Least Square (PLS) sebagai Metode Alternatif Sem Berbasis Varians (LISREL) Dalam Eksplorasi Data Survey Dan Data Mining," *Telematika*, vol. 7, pp. 1–3, 2015.
[15] R. H. Hoyle and A. T. Panter, "Writing about structural equation models," *Struct. Equ. Model. Concepts, issues, Appl.*, no. September, pp. 158–176, 1995, [Online]. Available: http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=1995-97753-009&loginpage=Login.asp&site=ehost-live.
[16] G. Hofstede and G. J. Hofstede, "Report on the organizational culture," pp. 1–44, 2018.
[17] P. Pavlou and L. Chai, "What Drives Electronic Commerce across Cultures? A Cross-Cultural Empirical Investigation of the Theory of Planned Behavior.," *Jounal Electron. Commer. Res.*, vol. 3, no. 4, pp. 240–253, 2002, [Online]. Available: http://www.jecr.org/sites/default/files/03_4_p04.pdf.
[18] N. Janićijević, "The Impact of National Culture on Leadership," *Econ. Themes*, vol. 57, no. 2, pp. 127–144, 2019, doi: 10.2478/ethemes-2019-0008.
[19] Bernhard Tewal, "Organizational Behaviour," 2017.