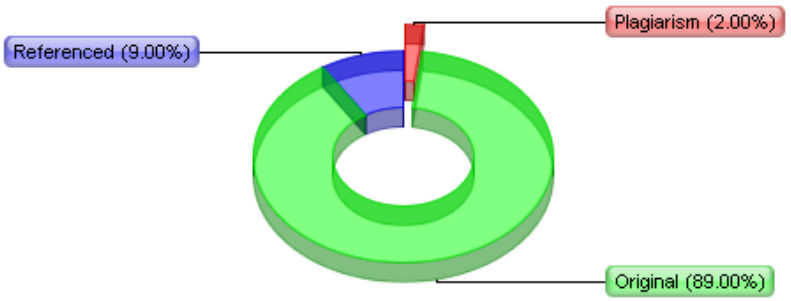
Plagiarism Detector v. 1092 - Originality Report:

Analyzed document: 23/06/2019 10:02:10

"IMPROVING SECURITY AWARENESS OF INFORMATION - BAHAN JURNAL CAKRAWALA PENDIDIKAN.docx"

Licensed to: **Iffah Budiningsih**

Relation chart:



Distribution graph:

Comparison Preset: Word-to-Word. Detected language: Indonesian

Top sources of plagiarism:

% 6	wrds: 302	https://www.researchgate.net/publication/332869494_The_Level_of_Information_Security_Aware...
% 6	wrds: 302	https://www.researchgate.net/publication/332869494_The_Level_of_Information_Security_Aware...
% 5	wrds: 256	https://www.researchgate.net/publication/317606573_An_Assessment_of_the_Level_of_Informati...

[Show other Sources:]

Processed resources details:

202 - Ok / 38 - Failed

[Show other Sources:]

Important notes:

Wikipedia:	Google Books:	Ghostwriting services:	Anti-cheating:
[not detected]	GoogleBooks Detected!	[not detected]	[not detected]

Excluded Urls:

Included Urls:

Detailed document analysis:

IMPROVING
SECURITY AWARENESS of
INFORMATIONIffah Budiningsih
1, Tjiptogoro Dinarjo Soehari 2, Irwansyah31
Faculty of Teaching and Educational Sciences As Syafi'iyah Islamic University, Jakarta - Indonesia, e-mail: mailto:iffah_budiningsih@uia.ac.id
iffah_budiningsih@uia.ac.id2
Magister Management Programe of Mercubuana University, Jakarta- Indonesiae-mail: mailto:tjiptogd@yahoo.com
tjiptogd@yahoo.com3
Magister Managemen Progame of Mercubuana University, Jakarta -Indonesia, e-mail: mailto:ironesyah.umb@gmail.com
ironesyah.umb@gmail.comAbstract
The advancement of science and technology, especially in the field of Information and Communication Technology (ICT) is characterized by the availability of information access anywhere, anytime, and by anyone; faster and easier process of sending and processing information. On the other hand, behind the convenience offered by ICT contains vulnerabilities (security gaps) that make it easier for unauthorized parties to try to steal (tap) and modify information.

Plagiarism detected: **0,24%** https://www.researchgate.net/public... + 4 more resources! id: **1**

The purpose of this study is to examine the factors that influence the

level of information security awareness. The research method used is the explanatory quantitative influence of independent variable perceptions of supporting organizations (X1), competence (X2) and motivation (X3) and the dependent variable is information security awareness (Y). Data analysis used multiple regression & correlation analysis, and the sample was taken 140 people proportionally stratified random sampling from the target population as many as 324 people. The results of the study are: 1) the model of improvement / strengthening

Plagiarism detected: **0,11%** https://www.researchgate.net/public... id: **2**

of information security awareness can be

predicted using the equation Y = 1.918-0.137X1+0.512X2+0.209X3; 2) the competence is the dominant factor that influences the information security awareness compared to the perceptions of supporting organizations and motivation; 3) the perception of supporting organizations and motivation are factors that can be ignored, because those do not have a significant effect on efforts to increase information security awareness; 4) the information security awareness can be improved by improving the competence of employees continuously & tiered; 5) model instructional

Quotes detected: **0,04%** in quotes: id: **3**

"Awareness Training"

developed by Milliam Schutz can be used to improve the attitude/character of information security awareness.
Keywords: information security awareness, perception support of organization, competence, motivation Abstra kKemajuan ilmu & teknologi, khususnya di bidang informasi dan comunikasi teknologi (Information & Communication Technology/ICT) yang ditandai, antara lain: ketersediaan informasi di mana saja, kapan saja dan oleh siapa saja; proses pengiriman informasi lebih cepat dan lebih mudah, tetapi di sisi lain di samping kenyamanan yang ditawarkan oleh ICT berisi kerentanan (celah keamanan) yang membuatnya lebih mudah bagi pihak yang tidak sah untuk mencoba mencuri(menyadap) dan memodifikasi informasi. Tujuan dari penelitian ini adalah untukmenguji/mengetahui faktor-faktor yang dapat digunakan untuk membangun tingkat kesadaran keamanan informasi. Metode penelitian yang digunakan adalah metode survei kuantitatif pengaruh variabel independen persepsi mendukung organisasi (X1), kompetensi (X2) dan motivasi (X3) terhadap variabel dependen kesadaran keamanan informasi (Y). Analisis data menggunakan analyisis korelasi & regresi jamak, sampel diambil sebanyak 140 orang secara proporsional stratified random sampling dari target populasi sebanyak 324 orang. Hasil studi: 1) model membangun kesadaran keamanan informasi dapat diprediksi dengan menggunakan persamaan Y = 1.918-0.137 X1 + 0.512 X2 + 0.209 X3; 2) kompetensi adalah faktor dominan yang mempengaruhi kesadaran keamanan informasi dibandingkan dengan persepsi mendukung organisasi dan motivasi; 3) persepsi mendukung organisasi dan motivasi yang faktor yang dapat diabaikan, karena mereka tidak memiliki efek yang signifikan pada upaya untuk meningkatkan kesadaran keamanan informasi; 4) kesadaran keamanan informasi dapat ditingkatkan melalui peningkatan kompetensi karyawan secara kontinyu dan berjenjang; 5) model pembelajaran Awareness Training yang dikembangkan oleh Milliam Schutz dapat digunakan untuk meningkatkan sikap/karakter

Quotes detected: **0,06%** in quotes: id: **4**

"kesadaran pengamanan informasi"

. Kata kunci: kesadaran
keamanan informasis, persepsi dukungan dari organisasi, kompetensi, motivasi, INTRODUCTION
Development in science and technology, especially in the sector of information and communication technology (hereinafter will be referred to as ICT) in this 21st century has led to a shift in

Plagiarism detected: **0,11%** https://www.scribd.com/presentation... id: **5**

the dynamics of culture and human

civilization. This phenomenon is shown by the ease of access to information regardless of the time and spaces by everyone and the implementation of computing machine capable of handling automatic routine activities anytime. In this globalized era, information can easily be accessed through various media, e.g., cable television, mobile phone, computer, laptop and the internet. One of the examples is the use of a search engine; this system helps people search real-time references in an affordable way. In addition,

Plagiarism detected: **0,11%** http://ehandbooks.dadeschools.net/p... + 6 more resources! id: **6**

the use of electronic mail or

email enables a person to collaborate with others effectively without leaving their workplace. Asabere and Samuel (2012) define term information and communication technology or ICT as the tool, facility, process, and equipment providing a particular environment with a physical infrastructures and facilities to generate, transmits, process, store and distribute information in many forms, including audio, text, data, chart and video. ICT is not only used for the private individual, but also for broader purposes or sectors, such as commercial (e-commerce), government (e-government), education (e-education), banking (e-banking), security and defense, health, and politics.In an article entitled Technology as a Threat to Privacy: Ethical Challenges to the Information Profession, Britz (2014) opines that although ICT has played a major role in processes, such as collecting, storing, extracting and distributing information; this may increase the potential of information accessibility and manipulation.This problem also leads to simultaneous and broader access to information; in other words, such an issue allows people to look for information about other individuals or organizations illegally. The utilization of ICT, despite its vulnerability that leads to information misuse through ICT wares, accelerates the distribution of information distribution. Stalling (2003) mentions several possible threats that harm the ICT system; those are (1) interruption, i.e., attacks that result in a breakage of a system; (2) interception, i.e., illegal access to information committed by unauthorized-one of the examples is wiretapping; (3) modification, i.e., an illegal act of changing asset or information by unauthorized; (4) fabrication, i.e., attaching false objects, such as email, into a computer network. Recently, website hacking, tapping government's communication, stealing and leakage of strategic data are among the major threats of the gov
ernment's information security. According to data by the Ministry of Communication and Informatics in the website http://teknologi.news. viva.co.id/, government websites (with a go.id domain) are the common targets for website hackers. It is revealed that the number of cyber-attacks in Indonesia has reached 36.6 million in the past three years (http://tekno.kompas. com/read/2013/10/17/0811211/Serangan.Cyber.Dunia.http://

Referenced: **0,15%** in: http://tekno.kompas.com/read/2013/10/17/0811211/Serangan.Cyb... id: **7**

tekno.kompas.com/read/2013/10/17/0811211/Serangan.Cyber.Dunia.Terbanyak.dari.Indonesia

Terbanyak.dari Indonesia). External threats to information security are probably from the internal of the institutions. This blames the failures of government employees in monitoring information leakage. An example of this case in leakage of research result and information of potential mining area; this ultimately attracts foreign investors to invest in the area. Information owned by regional or local government has commonly been the subject to cybercrimes as the system of the institution is yet managed professionally.. The employee who are responsible for the operation of information security, play an important role in planning and implementing information security system must be profesional; for that ' employees who handle information system ' should have been provided with competence in the field of 'information security ', through a variety of education in the field of information security. The number of establishments mainly in developing countries have not been optimal in the security management of a variety of important information. The major constraint the fact that some of its

Plagiarism detected: **0,11%** https://searchsecurity.techtarget.c... id: **8**

employees do not fully understand information

that needs more security, the way to secure it, and the process to classify whether the information is confidential, limited, or common. Many of the employees argue that

Quotes detected: **0,11%** in quotes: id: **9**

"there is no such confidential information"

in the era of information openness. This paradigm has resulted in poor management of strategic information of the many institutions specifically its security system to the point that the issue of confidential information leakage is inevitable. Misconception regarding types of information that needs more concern involves the aspect of security,

classification of the information, and procedures of securing. Another point worth considering is the fact that data security and confidential receive less attention from the employees. Such a negative attitude indicates that

Plagiarism detected: **0,11%** https://www.researchgate.net/public... id: **10**

the information security awareness of the

employees is still low. Information security awareness, mentioned in National Institute of Standars and Technology/NIST (2003), has a significant role as it serves as the starting point for all human resources in an organization to understand the concept of information and technology security. Competency of employees in managing information system is crucial to effectively implement the process of information security as this responsibility basically requires a high level of ICT competency. The implementation of Regulation of Electronic Information and Transaction has forced the employees, users, and management of information system to comprehend the points within the regulation. Palan (2007: 6) defines the term competency as the basic character of an individual that reflects his or her personality, self-concept, value, knowledge, and skill in a wide range of situation. Such characteristics remain for a long time as those are capable of enhancing performance in the workplace. Based on data from the institution where the research was conducted, show that the qualifications of the employee competency information systems handle as much as 86.76%

Plagiarism detected: **0,13%** https://www.justice.gov.uk/courts/p... id: **11**

does not yet have a certificate of

' expert ' managing information (see table 1)Table 1 Competency Of Information Management Staffs No.
Qualification/competency of Information Management Staffs
Percentage
(%)
1.
Yet certified as information management
86.76%
2.
Rank I Information Management Clerk
10.29%
3.
Rank II Information Management Clerk
4.65%
4.
Rank III Information Management Clerk
0.31%
Source: Processed Data 2013The result of a study by Casmir (2005) concludes that the causes of problems regarding information security are lack of management support, poor information security awareness, lack of motivation and training related to information security, and lack of communication. The above discussion functions as the grounding of this present study to investigate the most prominent factors in raising information security awareness (dependent variable). The variable of this study involves the independent variables only, consisting of perception of organizational support, competency, and motivation of the employees in information management
METHODOLOGY
This survey research is to examine and analyze the influence of organizational support perception (X1), competency (X2) and motivation (X3) on information security awareness (Y). A regression analysis was used to determine the correlational model among variable X1, X2 and X3, and variable Y altogether. Furthermore, the correlational analysis was to determine the significant correlation between the independent variables and the dependent variable. The population in this study involved 324 employees responsible for managing information system in Goverment Institution and the sample are 140 employees were selected as the sample using proportionate stratified random sampling.

Plagiarism detected: **0,11%** https://www.researchgate.net/public... id: **12**

The data were collected using a

non-test instrument (questionnaire) and Likert scale related to the optimization of the information system; the scale ranges from 1 to 5 with the description: 5 = highly agree, 4 = agree, 3 = neither agree nor disagree, 2 = disagree, and 1= highly disagree. The result of this research was analyzed using descriptive analysis (central tendency) and inferential analysis (correlational and multiple linear regression analysis); a software SPSS for Windows was also utilized to analyze the data. Variable & Indicator
s of ResearchThe variable consisted of the dependent variable (Y), i.e., information security, whereas the independent variables comprised organizational support perception (X1), competency (X2), and motivation (X3) with the equation as follows:Y = a + bX
1+ cX2+ dX3+ €The information regarding the indicator
s of the variables of research is depicted in the following Table 2. Table 2 Indicators of Research VariablesNo

Variables
Indicators
1
Information Security Awareness (Y)
Aware of the roles and responsibilities of the employees
Aware of risks if abiding the rules
Understanding the rules/policy
Understanding the procedures
2
Perception of
Orga-nizational Support (X1)Reward by the organization
Supportive work atmosphere
c. Perception of supports of the superior
d. Fairness/transparency of the procedures
3
Competency (X
2)Attitude
Knowledge
Skill
4
Motivation (X
3)Internal (being committed to achieve excellence, to response work challenges, and to succeed) External (transparency of procedure, acknowledgment, salary, work condition) Validity and Reliability Test of Research Instrument
Testing the instrument on 20 respondents was conducted firstly before using it during the next phase. This is to examine its validity using the r formula of Pearson Product Moment. The r formula of Cronbach Alpha was also used to test the instrument's reliability. The result of validity test of variable Y (information security awareness) and independent variables X1 (organizational support perception), X2 (competency), and X3 (motivation) are depicted in Table 3 as follows. Table 3 Results of Instrument Validity And Reliability Test of Y, X1, X2 and X3 VariableNo.
Variable
sTotal of Valid Instrument
r-Count (Pearson) Value
Reliability Coefficient
Description
1
Information Security Awareness (Y) 16
0.302 - 0.769
0.866
Valid & Reliable
2
Perception of Organizational Support (X
1)16
0.365 - 0.780
0.891
Valid & Reliable
3
Human Resource Competency (X
2)23
0.308 - 0.811
0.913
Valid & Reliable
4
Human Resource Motivation (X
3)21
0.337 - 0.732
0.857
Valid & Reliable
RESULTS AND DISCUSSION
Results
Requirement analysis testing, i.e., normality and homogeneity test was conducted prior to multiple correlations and regression analysis. In this study, both requirement analysis has been satisfied, where the data of the variable Y, X1, X2, and X3 is normally distributed, and whereas the variable Y over the variables X1, X2 and X3 are homogeneous.

The analysis on the correlation of organizational support perception (X1), competency (X2) and motivation of human resources (X3) reveals that these variables along with the variable of information security awareness (Y) results in the multiple coefficient correlation value R = 0.550 (see Table 3.1). This shows that there is a positive and significant correlation among the independent variables and the dependent variable. Furthermore, the value of the determinant coefficient (R square) arrives at 0.302. In other words, the percentage of the contribution of the three independent variables, i.e., organizational support perception (X1), competency (X2) and motivation (X3) on information security awareness (Y) reaches 30.20%, and the remaining 60.80% refers to other factors. The overall result of the analysis of multiple correlation analysis and determinant coefficient using SPSS program is provided in the following Table 4.

Table 4

Multiple Correlations Coefficient X1, X2, X3 & YModel

R

R Square

Adjusted R Square

Std. Error of the Estimate

Change Statistics

F Change

df1

df2

Sig. F Change

1

.550

a.302

.287

.34401

19.615

3

136

.000

The result of ANOVA regarding the correlation of the organizational support perception (X1), competency (X2) and motivation (X3) on information security awareness (Y) is provided in Table 5 and Table 6.TABLE 5 ANOVAbModel

Sum of Squares

D

fMean Square

F

Sig.

1

Regression

6.964

3

2.321

19.615

.000

aResidual

16.095

136

.118

Total

23.058

139

a. Predictors: (Constant), X

3, X2, X1b. Dependent Variable: Y

Table 6 CoefficientsModel

Unstandardized Coefficients

Standardized Coefficients

T

Sig.

Correlations

B

Std. Error

Beta

Zero-order

Partial
Part
1
(Constant)
1.918
.365
5.259
.000
X
1-.137
.078
-.162
-1.751
.082
.107
-.148
-.125
X
2.512
.090
.486
5.699
.000
.531
.439
.408
X
3.209
.121
.180
1.728
.086
.340
.147
.124
The formula based on the result of ANO
VA from Table 5 and Table 6 regarding the correlation of the organizational support perception (X1), competency (X2) and motivation (X3) on information security awareness (Y) is as follows:Y =
1.918 - 0.137 X1 + 0.512 X2 + 0.209 X3The result of significance test on regression constants regres
sion is a = 1.918 (see Table 6), categorized

Quotes detected: **0,02%** in quotes: id: **13**

"significant"

as the value of sig 0.05 (0.000 0.05). In other words, the constants in that model significantly affect the level of information security awareness. The result of significance regression correlation analysis of X1 is b = -0.137 (see Table 6), 'not significant', due to the value of sig 0.05 (0.82 0.05). The result of significance regression correlation analysis of X2 is c = -0.512 (see Table 6), categorized 'significant', due to the value of sig 0.05 (0.00 0.05)

Plagiarism detected: **0,09%** https://northernbaldibis.blogspot.c... + 2 more resources! id: **14**

. On the other hand, the

result of significance regression correlation analysis of X3 is d = -0.209 (see Table 6) fall under 'not significant' category since the value of sig 0.05 (0.86 0.05). These results indicate that only the variable of competency (X2) affects

Plagiarism detected: **0,11%** https://www.researchgate.net/public... + 3 more resources! id: **15**

the level of information security awareness

(Y) and the other variables, i.e., organizational support perception (X1) and motivation of human resources (X3) do not affect variable Y. The result of significance test on the simple multiple regression analysis is Y = 1.918 - 0.137 X1 + 0.512 X2 + 0.209 X3, categorized 'significant' as the value of sig, 0.00, is less than 0.05 (see Table 5). Furthermore, such a result also signifies that the model

Plagiarism detected: **0,11%** https://www.researchgate.net/public... id: **16**

can be used to determine the

extent to which the information security awareness has achieved using the data of variable X1, X2, and X3 if all of the independent variables have been identified. The multiple linear regression model Y = 0.137 + 0.512 X2 + 0.209 X3 + 0.208 X3 indicates that if the factor of competency (X1) and motivation (X2) score 2 (good category), the result score of the information security awareness is = 1.918 + 0.137 (2) + 0.512 (2) + 0.221 (2) = 1.918 + 0.274 + 1.024 + 0.418 = 3.086 or falls under sufficient category; the standard

of the level of information security awareness

is at least all the constants arrive at score 4 (good) or 5 (very good). The variable of organizational support perception (X1) and motivation (X2) 'can be ignored' as these variables do not significantly affect

the level of information security awareness of

the employees (the result of regression coefficient test Table 6). This suggests that only the aspect of 'competency' that dominantly affects the level of information security awareness. The model also signifies that the information security level of the employees in the research site arrives at 1.928 or poor category if all variables X1, X2, and X3 score 0. Therefore, the competency of the employees in the research site must be improved to reach the standard score, i.e., 4 or 5 (good or very good category). This effort must be actualized continuously and in line with the development of ICT.Discussion

All of the employees (the respondent of this research) are civil servants who have, without question, passed a particular standard during the recruitment process. Basically, there are personal traits related to civil servants, i.e., To have

the responsibility to provide quality services to society;To have

motivation to secure financial future; To have for limited funding or resources in their job, and;The significant depending on external resources due to exporting resources in managing the information; sehingga SDM These characteristics ha

ve contributed to the result of this present study that the only element that significantly affects the information security awareness is the employees' competency. Such a result implies that the employees should continuously enhance their competency by participating in seminars, workshops, discussions, training, on-the-job training, and benchmarking or visiting other institutions. Low information security awareness of the employees has drawn the attention of Institution leaders will the importance of the roles and functions of a special unit in information security. Most of the officers in addition to the competence of managing information systems are not yet in compliance with minimum standards, also because ' facilities and infrastructure supporting information systems security are not optimal. Other things to get the attention of the leadership of the management that another issue is obstacles in the career development of the employees. Almost 75% of the employees managing the information system have worked for more than 10 years without being transferred to other work units. This gives a bad impact for the employees in question, namely the existence of a saturation work that would eventually emerge and demotivation impact on decreasing awareness of information security. Hassan, Saad et al. (2014) argue that perception of organizational supports reflect how a labor force feel towards the attention of his or her organization care and pay attention to its employees in the information system unit. A study by Rhoades and Eisenberger (2001) points out that an employee will consider him or herself being appreciated if the organization provides support to all its workforces. This situation drives the employee to improve his or her cooperation and performance. Furthermore, Rotter (as cited in Hjelle and Ziegler, 1992: 374-375) clarifies that human needs to attain certain goals or conceptualize values continuously arise for pursuing self-pleasure. That being said, one must functions such values as a driving force to attain a successful target. Rotter adds that the desire for pursuing one's needs is due to an expectation worth of certain values based on experiences in a compared situation. One of the fulfillments or aspects functioning to motivate an individual to work is a supportive external environment--this refers to everything that influences the needs of employees, yet the fulfilling such needs are beyond the capabilities of the employees. Some of the examples are organizational policy, administration or supervision procedures, interpersonal relationship, status, security, money or salaries, work condition, and appreciation on personal life. These examples affect the work motivation of employees. Competence to optimally operate information security devices in supporting information security is necessary. As is the case in the general elections in Indonesia in 2019 recently, the information management personnel were allegedly incompetent to operate various information security tools that ultimately produced less than optimal information in meeting the expectations of all parties. Stalling (2003) mentions several possible threats that

harm the ICT system; those are:1

.The interruption, i.e., attacks that result in a breakage of a system; 2

. The iterception, i.e., illegal access to information committed by unauthorized-one of the examples is wiretapping; 3

. The modification, i.e., an illegal act of changing asset or information by unauthorized; 4

. The fabrication, i.e., attaching false objects, such as email, into a computer network. According to EB Taylor in Suherman et al. (2016: 82-83) that human factors as creators of culture are factors that influence the existence of information security threats, as in the following:Culture of mutual help: can be used as a gap to steal / intercept information, modify the information or insert information;

Knowledge: lack of knowledge so that they do not know that certain information is confidential; Trust: information is given to others on the basis of 'trust' that the person will not use the confidential information provided;Fear/emphasis: through ways to intimidate/threaten, one will easily divulge confidential information.Competence to handle/manage system information such as how the security device optimally can be done through a variety of training.
Iffah Budiningsih et al. (2017: 264-265) have pointed out that training is a possible approach to enhance the competency

Plagiarism detected: **0,11%** https://pdfs.semanticscholar.org/d4... + 4 more resources! id: **19**

of employees. It is revealed that

the competency of employee is improved 45.5% through training; the remaining 55.5% of the employees' competency can be enhanced by other factors, e.g., workplace, superior supports, rewarding system, and facilities and infrastructures. The notion seen in the research by Tjiptogoro, D.S., Iffah B., Bakdi (2017:566) supports the aforementioned argument by Iffah et al. that competency is the most strategic factor of human capital to promote better work performance. Perltier opinion (2005) in Gundu (2012) that security awereness refers to sharing information with educating, and training employees about risks to data, especially risks to the confidentiality, integrity, or availability of data, and about knowing what to do to protect it.In this study,

Plagiarism detected: **0,13%** https://www.infosec.ox.ac.uk/traini... id: **20**

a high level of information security awareness

is one of the indicators that is demanded by information management institutions. Siponen (2001) argues that information security awareness is a preventive measure that aims to establish security procedures and principles explicitly in the minds of all employees. This is important because each security technique can be misused or misinterpreted, so that increasing information security awareness is important and demands every employee who handles information systems in order to minimize errors and maximize the efficiency of security techniques. Another important element in efforts to increase information security awareness is the top management factor. Furthermore, according to Cline and Jansen (2004) in Choi, et al. (2006) state that the importance of the awareness of the security of information for decision-makers (leaders) is how the principles of information management can be implemented by all involved so that the success of information security performance is achieved. According to Islam, D. C. et al. (2016: 26), information security efforts can be made by providing education about information security awareness, such as socializing password management techniques.When someone is already familiar with something, it will automatically conceal information that is indeed confidential. Positive characters such as 'secretive ability' will be possessed by a person through a long process that is through continuous habituation. Thus character education that conceals information (private or public property) is an education that familiarizes good values (keeping something secret) in the child's life from an early age; and will be more effective if implemented through a model or example. As revealed by Seftyanto, D. et al. (2012: 888) that character is not brought from birth, but must be built and developed through a long and not instant process. Furthermore, Seftyanto, D. et al. Argued that to build the character of information security awareness, it is necessary to introduce early cryptographic security to children, namely science and art to maintain the confidentiality of information, which includes: authentication, data integrity, confidentiality, and non repudiation which is an application of mathematics. Sudjana in Hamzah Uno et al. (2012: 121): divides competencies into three aspects: a) cognitive; b) attitude and c) psychomotor; where all three are one interconnected/related competence that cannot be separated between one competency with another. 'The character of information security awareness is covered in the attitude aspect of competence.Milliam
Schutz in Hamzah Uno et al. (2012: 30-31) explains that the learning model

Quotes detected: **0,04%** in quotes: id: **21**

"Awareness Training"

developed could be used to increase the

Quotes detected: **0,07%** in quotes: id: **22**

"level of human consciousness"

. Schutz emphasized that the need for increased personal awareness through awareness training is an interpersonal training, namely understanding of individuals. This Awareness Training Model can be used to increase the level of information security awareness; the learning principle uses the theory of 'encounter', which is a model of learning that uses simple game methods to develop values: a) openness, b) honesty, c) self-awareness, d) responsibility, e) attention to oneself and others . The Awareness Training Model includes 2 (two) stages, including:Stage of submission of tasks and their completion: The instructor/teacher gives direction about the tasks that must be carried out and how to finish them;Discussion on how to do the tasks or analysis of the implementation of tasks (joint reflection on what has been done).Until today, the Awareness Training model is still rarely applied in schools; many simple games can be done for the purposes of implementing this model.

Plagiarism detected: **0,13%** https://www.researchgate.net/public... id: **23**

The results of the study show that

the application of this model can improve 'children's emotional development.'.CONCLUSIONS

Plagiarism detected: **0,13%** https://www.researchgate.net/public... + 3 more resources! id: **24**

The level of information security awareness of

the information security employees is depicted in the model Y = 1.918 - 0.137 X1 + 0.512 X2 + 0.209 X3;Employees' competency is crucial rather than organizational support perception and employees' motivation.The factor of organizational support perception and employees' motivation are not significant in raising information security awareness, and therefore ones can pay less attention to these.Participating in seminars, workshops, discussions, training, on-the-job training, and benchmarking or visiting other institutions are among the approaches to improve the competency

Plagiarism detected: **0,11%** https://www.strategy-business.com/a... + 2 more resources! id: **25**

of employees who are responsible for

managing information system.Information security awareness has a very 'important' role in actualizing better performance of employees (or civil servants) who manage information systems given the rapid advancement of ICT, especially the development of connectivity and information dissemination. That being said, efforts to increase the competency of the employees through training are absolutely necessary to reduce the potential risk of information security violations.To introduce
early aboaut bcryptographic security to children, namely science and art to maintain the confidentiality of information, which includes: authentication, data integrity, confidentiality, and un-repudiation which is an application of mathematicsSecurity
awereness means understanding that there is a potencial for some people to deliberately or accidentally steal, demage or misuse the data that is stored within a firms/institution's computer system

Quotes detected: **0,04%** in quotes: id: **26**

".Model instructional "

Awareness Training

Quotes detected: **7,25%** in quotes: id: **27**

" developed by Milliam Schutz can be used to improve the attitude/character of information security awareness.REFERENES
As
abere, Nana Yaw & Samuel Edusah Enguah. (2012). Use of Information & Communication Technology (ICT) in Tertiary Educationin Ghana: A Case Study of Electronik Learning (e-Learning). International Journalof Informationand Communication Technology Research, 2 (1), pp:62-68.Brit
z,JJ.(2014) .Technology As A Threat To Privacy: Ethical Challenges to the Information Profession. From http://web.simmons.edu/~chen/nit/NIT'96/96-025-Britz.html
http://web.simmons.edu/~chen/nit/NIT'96/96-025-http://web.simmons.edu/~chen/nit/NIT'96/96-025-Britz.html Britz.htmlBudiningsih, I. , Tjiptogoro D. S., & Masduki A.(2017). Increased Competency Through Training Intervention. International Journal of Applied Business and Economic Research, 15 (6), pp 264-265C
asmir, Respickius & Yngström, Louise. (2015). Towards a Dynamic and Adaptive Information Security Awareness Approach, Proceedings of the Fourth World Conferenceon Information Security education (WISE-4). Organized by IFIP Working Group11.8 (IT Security Education), Moscow, Russia. ISBN 5-7262-0565-0.Choi, Namjoo; Kim, Dan; & Goo, Jahyun. (2006). Managerial Information Security Awereness Impact on an Organization's Information Security Performance. Paper 4016 AMICS Proceeding.Gundu, Tapiwa . 2012. Towards an Information Security Awereness Process for Enggineering SMEs in Emerging : Disertations, University of Fort hare.H
assan, Saad.,et.al.(2014). Measuring the Impact of Perceived Organization Support, Psychological Empowerment and Rewards on Employee 'Satisfaction: Testing the Mediating Impact of Employee Engagement, World Applied Sciences Journal, vol.30 (5), pp: 652-660.Hjelle, Larry A. & Daniel J. Ziegler (ed)
. (1992).Personality Theories, New York: McGraw-HillInc.Islami, D. C., Khodijah Bunga I. H.& Candiawan. (2016). Awareness Information Security Employees X Bank in Bandung Indonesia, INKOM Journal, 10 (1), p19-26, from DOI: http://dx.doi.org/10.14203/j.inkom,428%20from
http://dx.doi.org/10.14203/j.inkom,428 from http://jurnal.informatika.lipi.go.id/index.%20php/inkom/article/view/428 http://jurnal.informatika.lipi.go.id/index. php/ inkom/article/view/428.National Institute of Standars and Technology. (2003). Special Publication (NIST SP) 80 -100, Information Securuty Handbook : A Guide for Manager.
Palan
. (2017).Competency Management : Techniques To Implement Competency-Based Human Resource Management To Increase The Competitiveness Of The Organization, Indonesia Language Edition, Jakarta: PPM.Rho
ades, L. & Eisenberger, R. (2002). Perceived Organizational Support: a Review of the Literature. Journal of Applied Psychology, 87(4), pp.698-714.Uno, Hamzah B., Iffah Budiningsih & Keysar Panjaitan .(2012) The Model of Instructional((Second ed.).Gorontalo:BMT Nurul Jannah. Seftyanto, Donny., Mega Apriani, Tony Haryanto. (2012, 12 Noveber).

The Role Of Algorithms "

Caesar Cipher" In Building The Character of

Plagiarism detected: **0,13%** https://www.researchgate.net/public... id: **28**

Information Security Awareness. Paper presented at the

National Seminar of Matematic & Matematic Education, FMIPA University State of Yogyakarta. from https://core.ac.uk/%20download/pdf/11067011.pdf
https://core.ac.uk/ download/pdf/11067011.pdf.S
iponen, Mikko T. (2000). A Conceptual Foundation for Organizational InformationSecurity Awareness. Jurnal of Information Managementand Computer Security.

Plagiarism detected: **0,13%** http://agile.vtt.fi/publications.ht... id: **29**

University of Oulu, Department of Information Processing

Science, Finland, 8(1), pp. 31-41.Suherman, Pujo Widodo, Dadang Gunawan. (2017). Effectiveness of Information Security Threats Fasing Social Engineering.
Asymmetric Warfare Journal, (Journal of Study Programe), 3 (1), pp 82-83 from http://jurnalprodi.idu.ac.id/index.php/%20PA/%20article/%20view/94

Referenced: **0,15%** in: http://jurnalprodi.idu.ac.id/index.php/%20PA/%20article/%20v... id: **30**

http://jurnalprodi.idu.ac.id/index.php/ PA/ article/ vi

ew/94.S
talling, William. (2003).Cryptography and Network Security: Principles andPractices. New Jersey : Prentice Hall.Tjiptogoro D. S., Iffah B., & Bakdi. (2017). Performance Improvement Through Human Capital Strategic for Civil Servant.International Journal of Applied Business and Economic Research, 15 (24), p. 566.ooOoo
16