DOMINANT FACTOR FOR IMPROVING INFORMATION SECURITY AWARENESS

Iffah Budiningsih[1*], Tjiptogoro Dinarjo Soehari[2] & Irwansyah[3]
[1]Universitas Islam As-Syafi'iyah, Indonesia,
[2,3] Universitas Mercu Buana, Indonesia
*e-mail: iffah_budiningsih@uia.ac.id

Abstract: The advancement of science and technology, especially in the field of Information Communication Technology (ICT), is characterized by the availability of faster and easier information access. However, the development is vulnerable to misconducts, e.g., information theft. This study aims to determine the relationship between perception of organizational support, competence, and motivation with information security awareness. The survey involved a population of 324 people information system employees working in local governments in 33 provinces; as many as 140 people were selected as the sample using stratified proportional random method. The data were collected using a questionnaire and were further analyzed using multiple regression. The results of the research show that (1) Information security awareness is influenced positively and significantly by the organizational support perception, competence and motivation. (2) The aspect of competence is the dominant factor that contributes to the information security awareness compared to the organizational support perception and motivation. (3) Information security awareness can be improved by competencies, knowledge, and skills. The study also reveals that instructional awareness training model developed by 'Schultz' is applicable to improve the attitude or character of information security awareness.

Keywords: ***information security awareness, organizational support perception, competence, motivation***

FAKTOR DOMINAN UNTUK MENINGKATKAN KESADARAN KEAMANAN INFORMASI

Abstrak: Kemajuan ilmu pengetahuan dan teknologi, khususnya di bidang Teknologi Informasi dan Teknologi (TIK), ditandai dengan ketersediaan akses informasi dengan cepat dan mudah. Namun demikian, pengembangannya rentan terhadap penyalahgunaan, misalnya pencurian informasi. Tujuan penelitian ini untuk menentukan hubungan antara persepsi dukungan organisasi, kompetensi, dan motivasi terhadap kesadaran keamaan informasi. Survei yang dilakukan melibatkan populasi sebanyak 324 orang pegawai sistem informasi pemerintah daerah di 33 provinsi; di mana sebanyak 140 orang terpilih sebagai sampel dengan metode *stratified proportional random sampling*. Data dikumpulkan melalui angket yang kemudian dianalisis dengan regresi ganda. Hasil penelitian menunjukkan bajwa (1) kesadaran keamanan informasi dipengaruhi secara positif dan signifikan oleh persepsi dukungan organisasi, kompetensi, dan motivasi. (2) Aspek kompetensi adalah faktor dominan yang berkontribusi terhadap kesadaran keamanan informasi daripada persepsi dukungan organisasi dan motivasi. (3) Kesadaran keamanan informasi dapat ditingkatkan dengan kompetensi, pengetahuan, dan keterampilan. Penelitian ini juga mengungkap bahwa model pembelajaran pelatihan kesadaran yang dikembangkan oleh 'Schultz' dapat diterapkan untuk meningkatkan sikap atau karakter kesadaran keamanan informasi.

Kata kunci: ***kesadaran keamanan informasi, persepsi dukungan organisasi, kompetensi, motivasi***

INTRODUCTION

Development in science and technology, especially in the sector of information and communication technology (hereinafter referred to as ICT) in the 21st century has led to a shift in dynamics of culture and human civilization. This phenomenon is represented by the ease of access to information regardless of the time and spaces. Further, the condition is also seen in the implementation of computing machines capable of handling automatic routine activities anytime, regardless of its users. In this globalized era, information can be easily 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 affordably.

In addition, the use of electronic mail or email enables a person to collaborate with others effectively without leaving their workplace. Asabere & Enguah (2012) define term information and communication technology or ICT as the tool, facility, process, and equipment providing a particular environment with physical infrastructures and facilities to generate, transmit, process, store and distribute information in many forms, including audio, text, data, chart, and video. ICT is not only used by a certain individual, but also by groups in some sectors, such as commercial (e-commerce), government (e-government), education (e-education), banking (e-banking), security and defense, health, and politics.

Although ICT has played a major role in processes, e.g., collecting, storing, extracting, and distributing information, Britz (1996) argue that such a situation may increase the potential of information manipulation. Stalling (2003) mentions several possible threats that harm the ICT system, namely (1) interruption, i.e., attacks that result in a breakage of a system; (2) interception, i.e., illegal access to information committed by unauthorized individual—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 and stealing information from the government's communication, and leakage of strategic data are among the major threats attacking the government's information security. According to data by the Ministry of Communication and Informatics, government websites (with a *go.id* domain) are the common targets of website hackers. Besides, external threats to information security are probably from the internal of the institutions. This situation blames the failures of government employees in monitoring the security system. An example of this case is the leakage of research results and information on potential mining areas; this ultimately attracts foreign investors to invest in the area. Information owned by local government has commonly been the subject to cybercrime that the system of the institution is yet managed professionally.

Employees who are responsible for the operation of information security play an important role in planning and implementing information security system must be professional; for this reason, those employees should master specific competence in the field of information security. They are expected to participate in various trainings. Such programs, however, are yet effective in developing countries. Another constraint is the fact that some of the employees do not have a grasp on areas that needs improvement. They also have no ideas regarding the difference between confidential, limited, or common information.

Many employees argue that "there is no such confidential information" in the era of information openness. This paradigm has resulted in poor management of strategic information specifically its security system in almost all institutions. Consequently, this issue causes information leakage. 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 the information security awareness of the employees is still low.

This research was conducted in 33 information security units of the local government in 34 provinces in Indonesia. The division serves to ensure the information security government and maintain the national security. Further, this work unit play a major role in implementing good management of information security and network security process of transmission of data or information into/out of the local government and the preparation of information security management policy in the local government.

Competency of employees in managing information systems is crucial to effective implementation. The process of information security 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 systems to comprehend all related regulations. Palan (2007) 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 situations. Such characteristics is considered as long-term skills. Based on data from the institution, 86.76% of the employees are yet certified as a professional in the field of information management (Table 1).

Table 1. Competency of Information Management Staffs (Crypto HR)

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	.31

Source: Crypto HR in 33 Local Government (2015)

In addition to the issues in the competence of managing information, many find that systems are yet in compliance with minimum standards. This situation blames poor facilities and infrastructure support for a security information system (limited budget). Another issue worth mentioned is employees' organizational leadership as most of them experienced some issues in their career development. Almost 75% of employees have more than ten years work experience without being promoted. These situations affect the information security awareness among the employees.

The result of a study by Casmir and Louise (2015) points out 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. Based on the above discussion, several problems related to information security among the local government serve as the focus of selecting the variables in this study. The variables are namely information security awareness, competencies of the management information system (knowledge, skills, attitude), organizational support perception and motivation.

In general, this research aims to find out the factors that affect the human capital strategy of information security awareness (Crypto HR) in the local government. The results of this study are expected to give input to the local government by which it enhances the information security awareness 'Crypto HR' and maintain the national security.

METHOD

This survey research is to examine and analyze the influence of organizational support perception (X_1), competency (X_2), and motivation (X_3) on information security awareness (Y). The research method used a survey with a population of 324 employees working in 'Crypto HR' in the local government offices within 33 provinces in Indonesia. As many as 140 of the employees were selected as the sample using a proportionate stratified random sampling. The data were from a questionnaire and it used a Likert scale; 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. Data analysis using multiple regression was to determine the model of the relationship between variables X_1, X_2 and X_3 with the Y.

Variable and Indicators of Research

The variable consisted of the dependent variable (Y), i.e., information security awareness, whereas the independent variables comprised organizational support perception (X_1), competency (X_2), and motivation (X_3) with the equation as follows:

$$\mathbf{Y = a + bX_1 + cX_2 + dX_3 + €}$$

The information regarding the indicators of the variables of research is depicted in Table 2.

Table 2. Indicators of Research Variables

No.	Variables	Indicators
1.	Information Security Awareness (Y)	a. Aware of the roles and responsibilities of the employees b. Aware of risks if abiding the rules c. Understanding the rules/policy d. Understanding the procedures
2.	Perception of Organizational Support (X_1)	a. Reward by the organization b. Supportive work atmosphere c. Perception of supports of the superior d. Fairness/transparency of the procedures
3.	Competency (X_2)	a. Attitude b. Knowledge c. Skill
4.	Motivation (X_3)	a. Internal (being committed to achieve excellence, to response work challenges, and to succeed) b. External (transparency of procedure, acknowledgment, salary, work condition)

Table 3. Results of Instrument Reliability Test of Y, X_1, X_2 and X_3 Variable

No.	Variables	Total Instrument	Reliability Coefficient (Variable)	Description
1.	Information Security Awareness (Y)	16	.866	Valid & Reliable
2.	Perception of Organizational Support (X_1)	16	.891	Valid & Reliable
3.	Competency (X_2)	23	.913	Valid & Reliable
4.	Motivation (X_3)	21	.857	Valid & Reliable

Table 4. General Description of Respondents

No.	Respondents' Identity	Number of Respondents (people)	Percentage
1.	**Sex:**		
	- Male	122	87.05
	- Female	18	12.95
2.	**Age (year)**		
	< 20	0	0
	20-30	15	10.72
	31-40	33	23.57
	>40	92	65.71
3.	**Education :**		
	- Senior High School	42	30.0
	- Diploma	4	2.86
	- Undergraduate	80	57.14
	- Post graduate	14	10.0
4.	**Working Tenure (year):**		
	< 1	1	7.14
	1-5	24	17.15
	6-10	18	12.86
	>10	97	69.26

Validity and Reliability Test of Research Instrument

The testing of the instrument was conducted before the distribution of the instrument to 20 respondents. This was to examine its validity using expert judgment and the r formula of *Cronbach Alpha*. Both of the formula were used to test the instrument's reliability. The result of the reliability test of variable Y (information security awareness) and independent variables X_1 (organizational support perception), X_2 (competency), and X_3 (motivation) are depicted in Table 3.

RESULTS AND DISCUSSION

Results

Some tests, e.g., normality, homogeneity, linearity, and multicollinearity tests were conducted before regression analysis. In this study, the data of the variable Y, X_1, $X_{2,}$ and X_3 are normally distributed, the variable Y over the variables X_1, X_2 and X_3 are homogeneous, variable Y is linear over X_1, X_2, X_3; and the value of tolerance X_1, X_2 and X_3 gets 1, meaning that the value of the VIF (Variance Inflation Factor) is below 10. In general, the characteristics of respondents of the research are presented in Table 4.

The result of regression analysis reveal that the determinant factor R square arrives at .302, meaning that the contribution probability of the three independent variables, i.e., organizational support perception (X_1), competency (X_2) and motivation (X_3) to information security awareness (Y) is 30.20%, and the remaining 69.80% refers to other factors. The overall result is presented in Table 5.

Table 5. Model Summary[a]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				Dubin-Watson
					F Change	df1	df2	Sig. F Change	
1	.550[a]	.302	.287	.34401	19.615	3	136	.000	1.815

a. Predictor: (Constant), X_3, X_2, X_1
b. Dependent Variable Y

Table 6. ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	6.964	3	2.321	19.615	.000[a]
	Residual	16.095	136	.118		
	Total	23.058	139			

a. Predictors: (Constant), X_3, X_2, X_1
b. Dependent Variable: Y

Table 7. Coefficients[a]

Model		Un-standardized Coefficients		Standardized Coefficients	t	Sig.	Correlations			Collinearity Statistics	
		B	Std. Error	Beta			Zero-order	Partial	Part	Tole-rance	VIF
1	(Constant)	1.918	.365		5.259	.000	-	-	-	-	-
	X_1	-.137	.078	-.162	-1.751	**.082**	.107	-.148	-.125	.597	1.675
	X_2	.512	.090	.486	5.699	.000	.531	.439	.408	.707	1.415
	X_3	.209	.121	.180	1.728	**.086**	.340	.147	.124	.471	2.125

a. Dependent Variable: Y

The result of Anova regarding the correlation of the organizational support perception (X_1), competence (X_2), and motivation (X_3) on information security awareness (Y) is provided in Table 6 and Table 7.

The formula, based on the result of Anova from Table 6 and Table 7 regarding the correlation of the organizational support perception (X_1), competency (X_2) and motivation (X_3) on information security awareness (Y), is:

$$Y = 1.918 - .137\ X_1 + .512\ X_2 + .209\ X_3$$

The result of significance test on regression constants regression is a= 1.918 (see Table 7), categorized "significant" as the value of Sig = .000 <.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 X_1 is b = -.137 (see Table 7), 'not significant', due to the value of Sig = - .082 > .05. The result of the significance regression correlation analysis of $X_2$is c= .512 (see Table 7), categorized 'significant,' due to the value of Sig = .00 > .05. On the other hand, the result of the significance regression correlation analysis of X_3 is d = .209 (see Table 7) fall under 'not significant' category since the value of Sig = .086 > .05. These results indicate that only the variable of competency (X2) significant affects the level of information security awareness (Y) and the other variables, i.e., organizational support perception (X_1) and motivation(X_3) affects but do not significant to variable Y.

The result of significance test on simultaneous the multiple regression analysis is $Y = 1.918 - .137\ X_1 + .512\ X_2 + .209\ X_3$, categorized 'significant' as the value F = 19.615 and Sig = .00 < .05 (see Table 6). Furthermore, such a result also signifies that the model used to determine the extent to which the information security awareness has achieved using the data of variable X_1, X_2, and X_3 if all of the independent variables are available. The variable of organizational support perception (X_1) and motivation (X_2) 'can be ignored' as these variables do not significantly affect the level of information security awareness (the result of the regression coefficient test see 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 X_1, X_2, andX_3 score is 0. Therefore, the competency of the employees in the research site must be achieved the standard score, i.e., 4 or 5 (good or very good category). This effort is actualizing continuously and in line with the development of ICT.

Discussion

The respondents of this research are employees (civil servants) in Crypto HR in the local government offices who are responsible for managing confidential information. There are general personal traits related to civil servants, such as 1) having the responsibility to provide quality services to society; (2) committed to secure financial future; (3) having limited funding or resources in their job, and; (4) depending on external resources in managing information. These characteristics have contributed to the result of this present study. The only element that affects information security awareness is the 'employee 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 visiting other institutions.

In this study, the organizational support perception is not significant to information security awareness. It is assumed that all government agencies share the same SOP. The organizational support perception is considered a supporting factor. Nevertheless, a specific is essential to increase the information security awareness as ICT changes over time. In some institutions, the role of organizational leadership/management is important. Cline & Jansen (2004) in Choi, Kim, & Goo (2006) state that the importance of the information security awareness for decision-makers (leaders) lies on how the principles of information management become applicable for all stakeholders to develop effective information security. Casmir & Louise (2015) adds that the problems caused by information security practices, including poor management support.

The present study also reveals that the the motivation factors of the employees in Crypto HR contribute to information security awareness. Almost 75% of the employees have worked for more than ten years without being transferred to other work units. In general, there are no issues in the aspect of employees' motivation.

Competence to optimally operate information security devices in supporting information security is necessary. This becomes an issue as in the recent 2019 election in Indonesia, the information management personnel were allegedly incompetent to operate various information security tools. All information systems are vulnerable to various threats for which it required skills to address the issue. According to Stalling (2003), threats to information systems encompass (1) the interruption, i.e., to attacks that result in a breakage of a system;(2) the interception, i.e., illegal access to information committed by unauthorized; (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.

Suherman, Widodo, & Gunawan (2017) discussed that human, as the source of cultural difference, is among the factors that influence the existence of information security. The examples of cultural threats are (1) misusing the idea of mutual help to steal information; (2) lack of knowledge in categorizing confidential information; (3) misusing confidential information; (4) intimidation in keeping confidential information. Siponen (2000) argues that information security awareness is a preventive measure that aims to establish security procedures and principles explicitly to all employees. This is important because each security is prone to misuse. Another important element in enhancing information security awareness lies on the top management factor. Furthermore, Islami, Bunga, and Candiawan (2016) state that information security can be made by providing education about information security awareness.

Competence to handle/manage system information, such as how a security device can be done through various training and short-courses. Doolet (Ashabugh, 2012) found that training is central to improving competence rather than performance enhancement. The notion seen in the research by Soehari, Budiningsih, & Bakdi (2017) supports the argument by Doolet that competency is the dominant factor of human capital to promote better work performance. Perltier (Gundu, 2012) opines that security awareness refers to sharing information through educating and training employees about risks of data confidentiality, integrity, and efforts to protect its security.

Positive characters, such as 'secretive ability' will be comprehended by a person through a long process or habitual practice. Thus, character education is important to promote the values of keeping confidential information. Wagiran, Pardjono, Suyanto, Sofyan, Soenarto, & Yudantoko (2019) opine that honesty is an important soft-skill of an employee. Moreover, Seftyanto, Apriani, & Haryanto (2012) an individual's character is not something a person born with. Character is something that should be built and developed through long processes. Seftyanto, et. al. (2012) argued that it is necessary to introduce early cryptographic security to children to introduce the concepts of confidential information, which encompasses (1) authentication, (2) data integrity, (3) confidentiality, and (4) non repudiation. These aspects are integrated in math subject.

Uno, Budiningsih, & Panjaitan (2012) agreed to divide competencies into three aspects: (1) knowledge, (2) attitude, and (c) psychomotor. All of these are interconnected/related competence. 'The character of information security awareness is involved in the attitude aspect of competence. Uno et al. (2012) explains the idea of Milliam Schutz that the learning model of "awareness training" is applicable to increase the "level of human consciousness." This signifies the need for improving personal awareness through interpersonal training. 'Awareness Training Model' can be used to increase the level of information security awareness; the learning principle uses the theory of 'encounter', i.e., a learning model utilizing simple game methods to develop values, such as (1) openness, (2) honesty, (3) self-awareness, (4) responsibility, (5) attention to oneself and others . The Awareness Training Model includes two stages, including (1) stage of submission of tasks and its completion: the instructor/teacher gives direction about the tasks that must be carried out and how to accomplish it; (2) discussing how to perform the tasks or analyzing the implementation of tasks.

Recently, only few schools have started to implement 'awareness training model' despite the simplicity of the model to incorporate simple games. The results of the study show that the application of this model can improve children's emotional development.

Implications

Competence is a dominant factor, so the focus of the policy is to secure information to increase the competencies that are instrumental in this research. **Knowledge: (**1) relevant educational background; **(**2) relevant work experience; (3) mastering of security information or coding; (4) understanding information security process; (5) mastering theories and application of coding; (6) mastering information security implementation: confidentiality, data integrity, and anti-tapping.

Skill: (1) skillfully operating coding equipment; (2) capable of overcoming coding equipment troubleshooting; (3) capable of managing coding tasks; (4) promoting effective and efficient coding equipment; (5) effectively and efficiently use all coding equipment; (6) addressing the organizational problems immediately; (7) capable of performing information security or coding tasks wherever needed.

Attitude: (1) ability to work effectively and efficiently in an emergency institution; (2) ability to adapt with a specific workspace; (3) ability to adapt in any situation; (4) interested in learning coding; (5) committed to study coding in advanced level; (6) following work ethics; (7) feeling of being good and worthy in in the field of coding; (8) appreciating the work of securing confidential information; (9) taking care of oneself to maximize personal tasks; (10) avoid discussing about coding with strangers.

CONCLUSIONS

Information security awareness is influenced positively and significantly by the organizational support perception, competence, and motivation; and the model of improvement of information security awareness can be predicted using the equation $Y = 1.918 - .137 X_1 + .512 X_2 + .209 X_3$. This signifies that the information security awareness can be improved by organizational support perception, competence, and motivation. Competence is the dominant factor that influences the information security awareness compared to the organizational support perception and motivation. The organizational support perception and motivation are not significant in raising information security awareness (small influence). The determinant factor $R^2 = .320$; it signifies that the contribution probability of the three independent variables, i.e., organizational support perception, competence, and motivation to information security awareness is 30.20%, and the remaining 69.80% refers to other factors.

The implications of this research are (1) to improve the competence of all employees including knowledge, skills, and attitude based on the implications mentioned earlier; and the model of 'awareness training'developed by Schutz can be used to improve the attitude/ character of information security awareness; (2) to introduce "cryptographic" security to children, through science and art learning to maintain the confidentiality of information, which includes authentication, data integrity, confidentiality, and non-repudiation. These are the applications of mathematics subject; (3) to promote shared understanding that information security awareness is prone to misuse and other misbehaviors.

REFERENCES

Asabere, N. Y. & Enguah, S. E. (2012). Use of Information & Communication Technology (ICT) in tertiary education in Ghana: A case study of electronic learning (e-learning). *International Journal of Information and Communication Technology Research*, *2*(1), 62-68.

Ashabugh, M. L. (2012). Expert instructional designer voices: Leadership competencies critical to global practise and quality online learning designs. T*he 35th Annual Proceedings-AECT,* 3-19.

Britz, J. J. (1996). Technology as a threat to privacy: Ethical challenges to the information profession. *Microcomputers for Information Management*, *13*(3-4), 175-193.

Casmir, R. & Louise, Y. (2015). Towards a dynamic and adaptive information security awareness approach. *Proceedings of the*

Fourth World Conference on Information Security education (WISE-4), Organized by IFIP Working Group11.8 (IT Security Education), Moscow, Russia.

Choi, N., Kim, D. J, & Goo, J. (2006). Managerial information security awareness impact on an organization's information security performance. *Proceedings of the Twelfth Americas Conference on Information Systems*, 3367-3375.

Gundu, T. (2012). *Towards an information security awareness process for engineering SMEs in emerging* (Doctoral Dissertations, University of Fort hare). Retrieved from https://pdfs. semanticscholar. org/74cc/5325a9bcc1f014ad022888749e23c35f0ac. pdf.

Islami, D. C., Bunga, K., & Candiawan. (2016). Awareness information security employees X bank in Bandung Indonesia, *INKOM Journal*, *10*(1), 19-26. doi:10.14203/j. inkom,428.

Palan, R. (2007). *Competency management: Teknik mengimplementasi manajemen sdm berbasis kompetensi untuk meningkatkan daya saing organisasi*. Jakarta, Indonesia: PPM.

Uno, H. B., Budiningsih, I. & Panjaitan, K. (2012). *Model Pembelajaran.* Gorontalo, Indonesia: BMT Nurul Jannah.

Seftyanto, D., Apriani, A., & Haryanto, T. (2012, November). *The role of algorithms "caesar cipher" in building the character of information security awareness*. Paper presented at the National Seminar of Mathematics & Mathematics Education, Universitas Negeri Yogyakarta, Indonesia.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Journal of Information Management and Computer Security*, *8*(1), 31-41. doi:10.1108/09685220010371394.

Suherman, S., Widodo, P., & Gunawan, D. (2017). Effectiveness of information security threats facing social engineering. *Jurnal Peperangan Asimetrik, 3*(1), 82-83.

Stalling, W. (2003). *Cryptography and network security: Principles and practices*. New Jersey, NJ: Prentice Hall.

Soehari, T.D., Budiningsih, I., & Bakdi, B. (2017). Performance improvement through the human capital strategy for civil servant*, International Journal of Applied Business and Economic Research*, *15*(24), 551-568.

Wagiran, W., Pardjono, P., Suyanto, S., Sofyan, H., Soenarto, S., & Yudantoko, A. (2019). Competencies of future vocational teachers: Perspective of in-service teachers and educational experts. *Cakrawala Pendidikan*, *38*(2), 387-397. doi:10.21831/cp.v38i2.25393.