*Advances in Social Science, Education and Humanities Research, volume 501*
**Proceedings of the 6th International Conference on Education and Technology (ICET 2020)**

# Design, Development, and Implementation of Information Security Education for Teachers and Educational Personnel's: Framework of Technology for Indonesia

Teguh Triwiyanto [1, 2, *], Suyanto [3], Lantip Diat Prasojo [3]

[1] *Department of Educational Management, Postgraduate, Universitas Negeri Yogyakarta, Yogyakarta, Indonesia*
[2] *Department of Educational Administration, Faculty of Education, Universitas Negeri Malang, Malang, Indonesia*
[3] *Post-Graduated School, State University of Yogyakarta, Yogyakarta, Indonesia*
** Corresponding author. Email: teguhtriwiyanto.2018@student.uny.ac.id; teguh.triwiyanto.fip@um.ac.id*

**Abstract**: This study was conducted to know about design, development, and implementation of information security education for teachers and educational personnel's: framework of technology for Indonesia. This study used qualitative method of analysis to find and understand central phenomenon's with kind of bibliography. The applicated method of data collecting was technic of gather and analyze the documents, conducted by technic of data mining with document analysis. The research results showed the components of education of information security integrated of categories of discussion consisting of design, development, and implementation. Design included categories of designs of methodology, safety, outsourcing, spreading, technological continuity, development process, and partners involvement and method of evaluation ready to be transferred (education). The components of development consisted of e-learning materials category supporting pictures/videos, security capacity, and continued professional development. The components of implementations were extra security actions, policy and framework of technology, and assurance curriculum of information security.

**Keywords**: design, development, implementation of information security education, teachers, educational personnel's

## 1. INTRODUCTION

Concerning about the importance of information technology and understanding who has to be responsible to protect assets of information could be started by knowing, understanding definition and key characteristics of information security, that could be conducted through education of information security (Infosec). Iqbal (2016) stated that the current education of information security has become increasingly important, developing the direct capability to overcome the challenges is precondition to diminish and make disappear the threat of cyber world. However, the existed studies showed that this field has rarely laboratories that were established pedagogically, which could be used flexibly to educate, to be used directly by students, teachers and educational personnel's, both in education units and online. The information security involves resources in organization that need to be well managed in forms of management and leadership.

Generating effective and efficient management and leadership on aspect of an information technology needs laboratory development to educate information security for teachers and educational personnel. Viewed from theory of education, design of laboratory development is generally utilized for learning process from theory of education. The steps consist of planning, implementation, and evaluation of learning process in laboratory for education. The studies conducted by Iqbal (2016) were perfecting conceptual model of laboratory of information security education by online and principles of early design and giving general instructions in direct training. This research has contributed by serving two main objectives. First, this research has suggested conceptual model of educational laboratory of information security education by online consisting of important entities: laboratory infrastructure, training (document), training of management, and EPI (Event Processing Interface). Second, this research has suggested principals of design to applicate conceptual models of

 

laboratory of information security education by online in different context of education.

In Indonesia, information security becomes the need of all units of education, it needs systematic paths of management to ensure sustainable effects, one of them could be reached through education of information security. Today, information security has been recognized as main subject in curriculum of information system (Ayyagari & Tyks, 2012)). The online learning has gotten popularity in sector of education (Allen & Seaman, 2010; Liu & Burn, 2007). Therefore, to meet the increasing need of information security specialists, many institutions, including universities have offered programs of Master in information technology for campus and online educations. The online education brings unique challenges (Allen & Seaman, 2010) such as how to design courses that could provide theoretical and practical knowledges, while the students are located in different places and time zones.

The implementation of information security is not as simple as the estimation. There are many challenges in design, development, and implementation of laboratory information security education. Chen et al., (2011) and Lim et al., (2010) stated that the problems such as accessibility to laboratory resource, secure communication, minimizing security risks introduced to students, isolating laboratories, scalability of laboratory, harmonizing pedagogically of laboratory activities, providing easy-to-use interface, handling problems related to backup and recovery, providing remote access, and problems of configuration.

The early literature view showed that the cost-effective virtual technology features have played important roles in making virtual laboratory to be popular. The facts of security instruments, both hardware's and software's, are expensive have made them to be strongly challenging for educational institutions in developing and maintaining their information security laboratories. This situation has caused platform development of server virtualization, Burd et al. (2011) and Lahoud & Tang (2006) stated that the development has included many servers, operating systems, and technic of virtualization. However, description of explicit design method or pedagogic approach adopted to design and develop the laboratories and related trainings has been largely ignored.

This study was conducted to know about design, development, and implementation of information security education for teachers and educational personnel's: framework of technology for Indonesia.

## 2. METHOD

This research used method of meta-analysis, reviewing several articles of international journals. The character of qualitative meta-analysis has aimed to find and understand central phenomenon's, by the types of literature. According to Berg & Lune (2017), in qualitative research the researchers must try to understand through symbol, ritual, social structure, social role, etc. The used approaches, according to the characteristics of qualitative research, such as stated by Dodgson (2017), not try to measure anything, therefore, assumption that there are objective ways to learn certain phenomenon's is not valid. The basic belief is there is a lot of different views about reality, depending on someone's perspective.

The research data sources are derived from literatures related to the discussed objects, in forms of books and journals. The primary source in this study was eight samples of articles of international journals concerning about education of information security. The articles were D'Arcy & Lowry (2019), Waag-Cowling & Leenen (2019), Okada et al. (2019), Ben Naseir et al. (2019), Dalton & Gronseth (2019), (H. Chen & Li, 2014), Morolong et al., 2019), and (Hentea et al., 2006).

The used method of data gathering was technic of collecting and analyzing various documents with technic of gathering and analyzing various documents with content analysis (Trilling & Jonkman, 2018), which was conducted using technic of text mining, by analyzing documents (Salloum et al., 2018).

## 3. RESULTS

The components of information security education for teachers and educational personnel consist cohesively from design, development, and implementation. The components of design of information security education are categories of methodological design, security, outsourcing, spreading, technological continuity, development process, and partners involvement and method of evaluation ready to be transferred (education).

The components of development consisted of categories of e-learning materials supporting pictures / videos, security capacity, and continued professional development. The components of implementations were extra security actions, policy and framework of technology, and assurance curriculum of information security. Table 1 shows the components of design, development, and implementation of information security education.

As technological framework in Indonesia, the education of information security for teachers and educational personnel's is a part of continued professional development with design and curriculum that could be transferred to domains of other subjects. The materials of information security education include outsourcing, spreading, and continued technology in digital economy, e-learning, cyber security; security of digital and cyberspace; implementation of extra security actions; and content of curriculum, methodology, currency, and research.

## 4. DISCUSSION

The components of design of information security education for category of methodological design of combination of cognitive and affective effects in education

need to be mastered by teachers and educational personnel's in units of education. D'Arcy & Lowry (2019) stated that model of discipline in tasks execution in organization with policy of information security could give the following benefits: (1) cognitive belief that is stable in consequences of discipline and indiscipline and affective construct based on nation: condition of positive, negative, and periodic moods, and security of events related to the job, and (2) conceptualization of expanded moral consideration and normative effects related to compliance to policy of information security of the employees.

**Table 1 Design, Development, and Implementation of Information Security Education**

| Components | Study Categories | References |
|---|---|---|
| Design of information security education | • Design of sampling methodology of experiences that is followed by statistic evaluation of hierarchy linear modeling.<br>• Design that is secure, *outsourcing*, spreading. And technological continuity in digital economy.<br>• Design of education where development process, partners involvement and method of evaluation could be transferred (education) to domains of other subjects. | (D'Arcy & Lowry, 2019)<br>(Waag-Cowling & Leenen, 2019)<br>(H. Chen & Li, 2014) |
| Development of information security education | • Development of e-learning materials supporting 360VR picturs/videos based on data of serucity education of IoT.<br>• Development of *cyber* security capacity.<br>• Development of continued professional through digital security and cyber. | (Okada et al., 2019)<br>(Ben Naseir et al., 2019)<br>(Dalton & Gronseth, 2019) |
| Implementation of information security education | • Implementation of extra security actions.<br>• Implementation of policy and technological framework.<br>• Implementation of effective security assurance curriculum needs content of curriculum, methodology, currency, and research. | (Morolong et al., 2019)<br>(Waag-Cowling & Leenen, 2019)<br>(Hentea et al., 2006) |

Waag-Cowling & Leenen (2019) stated that integration of technologies in digital condition has needed focus to be not only located in functional benefits but also to include and overcome the threats and challenges as investment in creating and maintaining conducive environment to get customer trust. Beaumont & Hartley (2019) stated that the lack of professional to fight with the growth cyber-attacks has demanded reactions from universities to provide the students with the relevant skills and knowledges.

In order that the information security education for teachers and educational personnel could be well implemented in units of education, it needs design of formation control, career development, development and improving competences, test of competence, redistribution according to prevailing regulation and could reach the fixed objectives needs supervision, monitoring, and evaluation. Therefore, weakness and occurred deviation in the field could be corrected and prevented so that it could produce professional teachers and they could manage the information security. These study results stated that the education of information security for teachers and educational personnel has been part of continued professional development with design and curriculum that could be transferred to domains of other subjects.

In Indonesia, there are several strategic issues underlying the frame of mind of design development of teachers and educational personnel to manage information security. The strategic issues are the existence of quantity and quantity imbalances of teachers and educational personnel between cities/regencies and between provinces. There is region with surplus, and there is also region with lacking. Therefore, it needs efforts of replacement according with the prevailing regulation. The teachers and educational personnel's development are not only related with quantity, but also with quality. In order to get professional teachers and educational personnel's in management of information security, it needs regulation concerning about appointment and design of development.

When the education is conducted emergently, such as at this moment, the pandemic which is stated by World Health Organization (WHO) as disease of coronavirus 2019 (covid-19), caused by severe acute respiratory syndrome of coronavirus 2 (sars-CoV-2), has stated as pandemic since 12 March 2020, the knowledge of information security becomes very much needed. The closure of all schools has made learning activities are conducted daringly, learning from home, and still using curriculum and materials such as normal condition.

The secure design, outsourcing, spreading, and continued technology in digital economy has become one of discussed studies in component of design of information security education. Model that could combine layers of cyberspace security in design of policy and frameworks of technology is very much needed by institution of education. Gamundani, Bhunu-Shava, and Bere (2019) have utilized model of plug and play that could be composed by the existing policy and framework to improve the process of digital decision making, D'Arcy & Lowry (2019) introduced model of employees compliance with policy of information security, Ma et al. (2019) introduced the using social media and identifying the factors that effect on user satisfaction with social media. In addition, this study could enrich practices of security education by

exploring the differences in security awareness related to user satisfaction. Nissenbaum et al. (2019) introduced models of Markov and Semi-Markov from quest real-time in education of information security.

Design of education where process of development and involvement with partners and method of evaluation could be transferred (education) to domains of other subjects, is one of design components of information security education. Beaumont & Hartley (2019)) developed scenario of learning based on opened access of problems that could be adapted, and developed together with partners of industry to provide students with relevant skills and knowledges. Hentea et al. (2006) stated that curriculum of education of information security assurance in units of education must be responsive to the needs of public population and industry where the graduates with skills and specialization in education of information security assurance have worked.

The study results have listed the components of development of information security education for teachers and educational personnel's which consisted of categories of e-learning materials supporting pictures/videos, security capacity, and continued professional development. Okada et al. (2019) stated that using new media such as 360VR picture/video could enable the electronic learning materials to get the students' interest. Elçi & Seçkin (2019) reminded that technology has many positive effects in education, but also has negative effects. One of the negative effects is the spreading cyberbullying from school limits to other social networks.

Security capacity shows that the threats to security of global cyberspace, including physical, personnel, and information, still go on to evolve and spread to highly connected world, regardless of international borders, both in detail and in scale of effects. Ben Naseir et al. (2019) stated that cyber-attacks could destroy the national stability, the increase has produced landscape of original global threats, and the developing magnitude of attacking mechanism has created "tsunami effect" in national cyberspace defenses. Paliszkiewicz (2019) stated that variables of trust (trust: competency, trust: policy; trust: integrity) have affected in predicting leadership of policy compliance of organizational information security. This finding is discussed and the implication of practices is analyzed.

This study results indicated that the continued professional development is very much needed by teachers and educational personnel's in units of education. Dalton & Gronseth (2019) stated that digital security and cyberspace are increasingly important focus for teachers to understand and learn how to manage, remember the current capacity of hacking, and could be implemented through pre-service training of teachers and continued professional development.

The development process is an inseparable part from planning of teachers and educational personnel. Process of development should refer to ratio, composition, qualification, and distribution of teachers and educational personnel's as result of need mapping. Ratio is a comparison of teachers and educational personnel's quantity with other things according to the provision. Qualification is requirements for position to fulfill the need of teachers and educational personnel. Whereas the inside composition and distribution are the spread of quantity and quality of teachers and educational personnel. The inside need of quality includes the need to manage the information security.

The implementation of information security education consists of the study related to extra security actions, policy and technological framework, and effective curriculum of information security assurance based on content of curriculum, methodology, currency, and research. Related with the implementation of extra security actions, H. Chen & Li (2014) stated that perception of appropriate demand – capability, perception of appropriate need – supply, and perception of appropriate value are effective to motivate the security commitment. Security commitment is partial mediator between complementary conformity (conformity between capability of demand and sufficiency of supply) and intention to participate and becomes full mediator between the additional conformity (conformity of value) and intention to participate. In addition, apathetic attitude would diminish motivation to involve in extra behavior, whereas value of conformity and commitment of security would eliminate the apathetic attitude.

Implementation of information security education for teachers and educational personnel's in unit of education needs concrete steps. The steps could be such as the followings: (a) need of technical guidance to make work programs of information security education; (b) need of educational program of wholly information security education could take care with the school and community needs, not only in provincial level; (c) need of suggestion from the ministry of education, provincial agency of education in form of letter to implement program of information security education; (d) need of monitoring and evaluation as activity control of program of information security education; (e) Supervisors need to accompany the schools to make program of information security education; and (f) need of training for teachers and educational personnel's in each region to improve program of information security education.

Implementation of policy and technological framework has indicated the future steps that are anticipative to the development of cyberspace, so that they could integrate them in policy. At this moment, framework and policy design of digital economy include components of cyberspace security in design of policy and framework of continued integration of digital technology. Bishop (2019) stated that organization, customer, and government must collaborate to develop standard and policy that supply prosperous environment for internet of things (IoT), mainly related to privacy and data security.

The study results showed that implementing effective curriculum of information security assurance needs content of curriculum, methodology, currency, and research. Hentea et al. (2006) stated that it is important to know that the contents of curriculum from program of education of information security assurance are multidiscipline, with the interrelated topics derived from computer science, computer technic, mathematics, management, system of information, business, politics, psychology, and law. The specific topics about critical infrastructure security must be included covering all sectors (agriculture, food, water, public health, emergency service, government, defense, information and telecommunication, energy, transportation, banking and finance, chemical industry and dangerous materials, post and shipping, monument and icon).

Curriculum is arranged to development of teachers and educational personnel's in order to get the assurance of information security by considering the balance of global, regional, national, and local developments. To answer the challenges, it needs direction of teachers and educational personnel's development according to the tasks of central technology and communications. The development of teachers and educational personnel's is effort to get qualified and competent teachers and educational personals in conducting their main jobs, with the skill of implementing information security. It needs facilitation in all regencies/cities/provinces by conducting development and mapping of teachers and educational personnel to optimize the capability of implementing information security assurance.

## 5. CONCLUSION

The component of design of information security education for teachers and educational personnel's category of methodological design of combination of positive and affective effects needs to be mastered by all citizens of organization of education units. The secure design, outsourcing, spreading, and continued technology in digital economy have become one of discussed studies in component of design of information security education.

Components of development of information security education for teachers and educational personnel consist of categories of e-learning materials supporting pictures / videos, security capacity, and continued professional development. As framework of technology in Indonesia, the education of information security is a part of continued professional development with design and curriculum that could be transferred to domains of other subjects. Implementations of information security for teachers and educational personnel consist of studies related with extra security actions, policy and technological framework, and effective curriculum of information security education based on content of curriculum, methodology, currency, and research.

## REFERENCES

[1] Allen, I. E., & Seaman, J. (2010). Learning on Demand: Online Education in the United States, 2009. In *Sloan Consortium (NJ1)*. Sloan Consortium. https://eric.ed.gov/?id=ED529931

[2] Ayyagari, R., & Tyks, J. (2012). Disaster at a University: A Case Study in Information Security. *Journal of Information Technology Education: Innovations in Practice*, *11*(1), 85–96.

[3] Beaumont, C., & Hartley, P. (2019). The Cyber Security Knowledge Exchange: Working with Employers to Produce Authentic PBL Scenarios and Enhance Employability. In Z. Pan, A. D. Cheok, W. Müller, M. Zhang, A. El Rhalibi, & K. Kifayat (Eds.), *Transactions on Edutainment XV* (pp. 209–228). Springer. https://doi.org/10.1007/978-3-662-59351-6_14

[4] Ben Naseir, M. A., Dogan, H., Apeh, E., Richardson, C., & Ali, R. (2019). Contextualising the National Cyber Security Capacity in an Unstable Environment: A Spring Land Case Study. In Á. Rocha, H. Adeli, L. P. Reis, & S. Costanzo (Eds.), *New Knowledge in Information Systems and Technologies* (pp. 373–382). Springer International Publishing. https://doi.org/10.1007/978-3-030-16181-1_35

[5] Berg, B. L., & Lune, H. (2017). *Qualitative research methods for the social sciences* (Ninth edition). Pearson.

[6] Bishop, S. (2019). The Internet of Things: Implications for Consumer Privacy Security. *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, 1–9. https://doi.org/10.1109/ICGS3.2019.8688024

[7] Burd, S. D., Gaillard, G., Rooney, E., & Seazzu, A. F. (2011). Virtual Computing Laboratories Using VMware Lab Manager. *2011 44th Hawaii International Conference on System Sciences*, 1–9. https://doi.org/10.1109/HICSS.2011.482

[8] Chen, F.-G., Chen, R.-M., & Chen, J.-S. (2011). A Portable Virtual Laboratory for Information Security Courses. *Advances in Computer Science, Environment, Ecoinformatics, and Education*, 245–250. https://doi.org/10.1007/978-3-642-23357-9_44

[9] Chen, H., & Li, W. (2014). *Understanding Organization Employee's Information Security Omission Behavior: An Integrated Model Of Social Norm And Deterrence*. *7*(2), 10=22.

[10] Chen, H., & Li, W. (2014). Understanding Organization Employee's Information Security Omission Behavior: An Integrated Model of Social norm and Deterrence. *PACIS*.

[11] Dalton, E., & Gronseth, S. (2019). *Best Practices for Teacher Educators to Address Digital Security Issues in Synchronous Sessions and Webinars*. 416–419. https://www.learntechlib.org/primary/p/207674/

[12] D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, *29*(1), 43–69. https://doi.org/10.1111/isj.12173

[13] Dodgson, J. E. (2017). Tentang Penelitian: Metodologi Kualitatif. *Journal of Human Lactation*, *33*(2), 355–358. https://doi.org/10.1177/0890334417698693

[14] Elçi, A., & Seçkin, Z. (2019). Cyberbullying Awareness for Mitigating Consequences in Higher Education. *Journal of*

*Interpersonal Violence*, *34*(5), 946–960. https://doi.org/10.1177/0886260516646095

[15] Hentea, M., Dhillon, H. S., & Dhillon, M. (2006). Towards Changes in Information Security Education. *Journal of Information Technology Education: Research*, *5*(1), 221–233.

[16] Iqbal, S. (2016). Design and Emergence of a Pedagogical Online InfoSec Laboratory as an Ensemble Artefact. *Journal of Information Systems Education*, *27*(1), 17.

[17] Lahoud, H. A., & Tang, X. (2006). Information security labs in IDS/IPS for distance education. *SIGITE '06*. https://doi.org/10.1145/1168812.1168826

[18] Lim, S., Oh, T. H., Choi, Y. B., & Lakshman, T. (2010). Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring. *2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, 327–332. https://doi.org/10.1109/SUTC.2010.61

[19] Liu, Y. C., & Burn, J. M. (2007). Improving the Performance of Online Learning Teams—A Discourse Analysis. *Journal of Information Systems Education*, *18*(3), 369–379.

[20] Ma, S., Zhang, S., Li, G., & Wu, Y. (2019). Exploring information security education on social media use: Perspective of uses and gratifications theory. *Aslib Journal of Information Management*, *71*(5), 618–636. https://doi.org/10.1108/AJIM-09-2018-0213

[21] Morolong, M., Gamundani, A., & Bhunu Shava, F. (2019). Review of Sensitive Data Leakage through Android Applications in a Bring Your Own Device (BYOD) Workplace. *2019 IST-Africa Week Conference (IST-Africa)*, 1–8. https://doi.org/10.23919/ISTAFRICA.2019.8764833

[22] Nissenbaum, O., Maro, E., Ishchukova, E., & Zolotarev, V. (2019). Markov and Semi-Markov Models of Real-Time Quests in Information Security Education. *2019 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, 221–224. https://doi.org/10.1109/USBEREIT.2019.8736621

[23] Okada, Y., Haga, A., Wei, S., Ma, C., Kulshrestha, S., & Bose, R. (2019). E-Learning Material Development Framework Supporting 360VR Images/Videos Based on Linked Data for IoT Security Education. In L. Barolli, F. Xhafa, Z. A. Khan, & H. Odhabi (Eds.), *Advances in Internet, Data and Web Technologies* (pp. 148–160). Springer International Publishing. https://doi.org/10.1007/978-3-030-12839-5_14

[24] Paliszkiewicz, J. (2019). Information Security Policy Compliance: Leadership and Trust. *Journal of Computer Information Systems*, *59*(3), 211–217. https://doi.org/10.1080/08874417.2019.1571459

[25] Salloum, S. A., Al-Emran, M., Monem, A. A., & Shaalan, K. (2018). Using Text Mining Techniques for Extracting Information from Research Articles. In K. Shaalan, A. E. Hassanien, & F. Tolba (Eds.), *Intelligent Natural Language Processing: Trends and Applications* (pp. 373–397). Springer International Publishing. https://doi.org/10.1007/978 -3-319-67056-0_18

[26] Trilling, D., & Jonkman, J. G. F. (2018). Scaling up Content Analysis. *Communication Methods and Measures*, *12*(2–3), 158–174. https://doi.org/10.1080/19312458.2018.1447655

[27] Waag-Cowling, N. van der, & Leenen, L. (2019). *ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS 2019*. Academic Conferences and publishing limited.