

How Inter-organizational Knowledge Sharing Drives National Cyber Security Awareness?: A Case Study in Indonesia

P.D. Persadha^{†*}, A.A. Waskita^{†‡}, M.I. Fadhila[†], A. Kamal[†], S. Yazid[†]

^{*}Communication and Information Security Research Center,
Jalan Moh Kahfi I no.88D Jagakarsa Jakarta Selatan, Indonesia

Email : pratama@cissrec.org

[†]Faculty of Computer Science, University of Indonesia,
Kampus UI Depok, Depok 16424, Indonesia

Email : setiadi@cs.ui.ac.id

[‡]Center for Technology and Safety of Nuclear Reactor, National Nuclear Energy Agency,
Kawasan Puspiptek Serpong, Tangerang 15310, Indonesia

Email : adhyaksa@batan.go.id

Abstract—Cyber security awareness is an essential factor in today's world as the threat of cyber attack keep raising due to many individuals, organizations, and government institutions depend heavily on cyber infrastructure. This make it apparent as well that there is a need to establish a framework to enhance inter-organizational collaboration to achieve national cyber security awareness. This proposed study outlines a planned inquiry towards the investigation of that relationship specific to the context of Indonesian country. Through the use of semi-structured interviews and empirical evidences from relevant literatures, the expected outcome of this research is to find the relationship between inter-organizational knowledge sharing and the creation of cyber security awareness behavior.

Index Terms—inter-organizational knowledge sharing, cyber security awareness, trust, communication, leadership, technology, rewards, education

I. INTRODUCTION

The current rapid development of information technology (IT) in Indonesia has contributed to the increasing number of parties, both individuals and organizations, that rely on cyber infrastructure [1]. A number of regions in Indonesia such as Surabaya [2], Bandung [3], and Jakarta [4] even have implemented e-government system. Ensuring cyber infrastructures and services running appropriately makes cyber security plays an important role in our todays activities.

Cyber security become an important factor to be considered today because it covers the human as potential target of attacks [5]. Schneier was also stated that "Only amateurs attack machines; professionals target people" [6]. Hence the cyber threats and the cyber attacks will be targeted to anything that give a larger impact to people, including

public services and critical infrastructures such as energy, water, transportation, and communication [7].

Meanwhile, the increasing popularity of social media, that can be seen from the increase of personal information sharing, storage, and processing, can cause a negative impact to the user in the case of violation of the security of personal information. One of the example of that violation is Phishing [8]. Because people are the ultimate goal of the cyber threat and cyber attack, then it is important for people to increase their awareness in cyber security in order to prevent victimization [9].

In our previous study [10], it was revealed that the structure of cybersecurity-related organizations in Indonesia are still overlapping each other. It can be seen from the aspect of their responsibilities. Also the role of non-governmental organizations in Indonesia seem like being under government supervision. This is different from the situation in Australia, where non-government organizations become equal partner to government organizations, both federal and state governments, in their cyber security framework. This conditions can be illustrated by Figure 1.

With the large numbers and sufficient capabilities, Indonesian society has the potential to become a pillar of the national cyber security. It can be seen from a number of their contribution to the development of IT in Indonesia [11], [12]. Indonesian society has also proved that they are capable of being a driving force for programs that benefit them through independent national community empowerment program (PNPM) [13]. A "bottom-up" collaboration model in a national cyber security has also been developed [14], and its implementation in Indonesia will be very beneficial. Basically cyber security is a collaborative works [15]. Thus establishing a cyber security awareness from collaborative knowledge sharing is a necessity to be applied

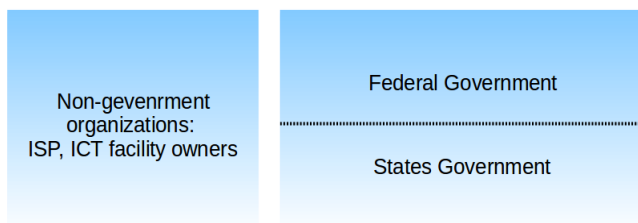


Fig. 1: Cyber security roles in Australia

in Indonesia.

In this paper, we propose a framework that is intended to increase collaboration among cyber-related communities in Indonesia, either individuals or organizations in the form of knowledge sharing. It is hoped that such collaboration will establish public awareness of cyber security. It's been motivated by the fact that anyone who interacts with the information technology can be a source of cyber space vulnerabilities. Then everyone must play a role in eliminating the occurrence of cyber security risks.

This paper will be organized as follows. After this introduction about the background of this study, we will discuss cyber security awareness in Sec. II. A review of the previous studies we presented in Sec. III. Next, our framework about inter-organizational knowledge sharing, which is the antecedent of the cyber security awareness and the expected finding from the research will be presented in Sec. IV. And the last section is the conclusion of our proposition.

II. CYBER SECURITY AWARENESS AND KNOWLEDGE SHARING

Situational awareness is a collective real understanding exist in an organization about the risks that should be faced [16]. While Endsley, as quoted by Webb et.al, defined the situation awareness as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" [17]. The ability to understand the risks is indispensable by each organization with the consideration of their information and control system [18]. On the other hand, the cyber threats or the cyber attacks was defined as any act by an insider or an outsider that compromises the security expectations of an individual, organization, or nation [19]. Then, we can conclude that the cyber security awareness is an understanding of the risks on the cyber space which may occur in each organization.

The understanding of the risks on the cyber space comes from the following steps [20] that are identifying and presenting the current situation, assessing that situation's impact/threat and projecting the situation and assessing the projection's impact/threat. The ability to appropriately identify the current situation is the most important step to anticipate the various risks that might be occurred. However, factors that affecting the cyber security risk are not

locally controlled and deliberately obscured. Consequently, to increase cyber security awareness requires consideration of technical, operational, business, and global or external factors [16]

At a certain time, organizations security level will be different to each other [21]. That is also occurred in Indonesia, the biggest archipelago in the world, where infrastructure, knowledge, and technology were not spread evenly across nation. And security breaches continue affecting many sectors, no matter how much the level of awareness [22]. Therefore, inter-organizational knowledge sharing should be developed, from which it can be expected that national cyber security awareness in Indonesia can be established. Knowledge sharing itself was defined as the activity to share, disseminate, and exchange knowledge, experience, skills, valuable information from one party to another party [23]. It can be delivered formally or informally, in the form of a written text, directly, or using electronic communication system.

Knowledge-sharing can include information about potential attacks, crime, and terrorism [24], that can help cyber related community to detect potential risks and prevent cyber attacks at an early stages [25]. This is also helpful to identify resources spread across a country [26]. Moreover, fusing the information and knowledge that were shared has also been studied to safeguard the critical infrastructure [27], [28]. The studies have been motivated by the fact that the cyber threats and attacks would compromise our daily life, because of the integration of information technology into today's system and the speed of the evolving cyber threats landscape. It was also shown that collaborating information between organizations with similar IT policies and strategies can improve detection rate of cyber attacks [29], [30]. Certainly, this will be very beneficial if the Indonesian people can realize it.

In this paper the term data, information, and knowledge sharing will be used interchangeably, although all three are substantially different [31].

III. LITERATURE REVIEW

One of the previous research that motivates us the most in proposing this paper is the research paper entitled "Organizational Culture and knowledge sharing : critical success factors", conducted by Al-Alawi et.al [32]. In that paper, Al-Alawi investigated organizational culture in the success of knowledge sharing such as interpersonal trust, communication between staff, information systems, rewards, and organization structure. And the most interesting factor from that paper is that it conducted in Bahrain, one of the Muslim dominated country, as Indonesia, in the world. From that research, Al-Alawi concluded that the previous factors were relate positively to knowledge sharing in organization.

Another research conducted by Chen et.al. also supports Al-Alawi. She concluded that inter-organizational

trust leads to better inter-organizational collaboration and knowledge sharing [33]. While Chen investigated manufacturing industry in Taiwan, where Chinese culture was dominant. She showed that the trust was the antecedent of inter-organizational knowledge sharing. It was also showed that inter-organizational knowledge sharing contributes primarily to sustaining the competitive advantage of the supply chain as a whole [34].

The next factor is communication. As previously described, knowledge can be shared by any means, any forms in any time among the stakeholder. Implicitly, knowledge can be shared if and only if communication can be constructed. An example from a case of higher education research conducted by Shabrina supports Al-Alawi in a communication factor. In that research, lecturer should increase communication among themselves to transform tacit into explicit knowledge [35].

In line with the trust factor, reward sometimes contributing to inter-dependencies pattern among stakeholder. At a certain time, one shares his/her knowledge to the others, while at the other time, he/she requires others. Šajeva concluded that psychological rewards were acknowledged to be important in fostering knowledge sharing [23]. And one of the psychological rewards is the sense of trust obtained from sharing the knowledge.

Santoro et.al. had also described network organization to represent cyber related inter-organizational collaboration, both government and non-government organization, where each person involved were organizing themselves to reach their common goals [36]. At this level, where common goals among stakeholder can be defined clearly, communication and trust must be established.

In the case of technical supporting factors, as described by Al-Alawi as information system, Mergel [37] showed that open collaboration has evolved as a new form of innovation creation with the support of GitHub [38]. GitHub that facilitate peoples, especially a community of government employees, in developing open source code and web development. Facilities that drive collaboration among student was also shown by Kim et.al research [39]. Connectedness among student in a class supported by web infused curriculum has motivate them to share their knowledge. Another similar case in Indonesia where supportive technology can drive user collaboration in a knowledge sharing activities is a technology that developed by ITB (Bandung Institute of Technology) to support teacher community in Bandung [40].

Another indispensable factor based on Al-Alawi research is organizational structure. We then hypothesize that there should be an entity that can be represented as a structure of the organization. Means that no matter what the structure of the organization is, knowledge sharing activities can be conducted. It is motivated by the fact that organizational structure of national cyber security in Indonesia still have a problem in the case of responsibility, as we

previously presented [10]. Al-Alawi was also presented that the problem usually exist in traditional organization as a bureaucratic structures which is slowing the processes and raising constraints on information flow [32].

It is also motivated by the fact that Indonesia is a masculine country that is sensible patriarchy [41]. For that reasons, we hypothesize that there should be an important role we mean as a leader. Leader is not only refers to a person who formally supervises other person or other organization, but also a person who are able to drive people to do something. Sobandi and Sudarmadji argued hypothetically that what makes collaboration happened is a good leadership [42]. In the context of cyber security, we will also investigate it.

From the literatures, leadership is also a components of a knowledge sharing. We can learn from Lunberg and Lidelöw [43] that a manager has a responsibility to show knowledge sharing behavior to construct a knowledge sharing culture. In another case, a teacher also plays an important role to enhance a knowledge construction collaboratively [44]. In a case of nuclear safety culture, leadership is also an important element to ensure the safety and secure operation of a nuclear facility [45]. Leadership roles was also studied by Aoyama et.al [46]. Besides their act as a driving force for the community, leader was also responsible in making decision. Ineffectivity in making a decision in handling a cyber incident will cause a shift in a control mode and ultimately cause an incident to be more difficult to be handled.

We also hypothesize that education plays an important role in a knowledge sharing behavior. Parsons et.al. were conducted a research that shows educational role [47]. He showed that knowledge of policy and procedures had a stronger effect on attitude towards policy and procedures. From that research, Parsons suggested that training and education will be more effective if it also provides an understanding of why information security is important.

IV. PROPOSED MODEL, PROPOSITIONS AND EXPECTED FINDINGS

From the literature review, this paper will investigate whether inter-organizations knowledge sharing can drive national cyber security awareness in Indonesia. If it is possible, we will also investigate how to realize it by using educational role. This paper will proposed similar to what Kathiravelu et.al. has proposed in the context of Malaysia [48], that are elements in constructing knowledge sharing.

This paper proposes the following proposition:

P 1: There is a strong relationship between inter-organizational knowledge sharing and cyber security awareness culture among country members.

The model of our proposition is illustrated in Fig. 2. We add education as a knowledge sharing element from Kathiravelu model, while changing organizational structure into leadership from Al-Alawi model. As the biggest

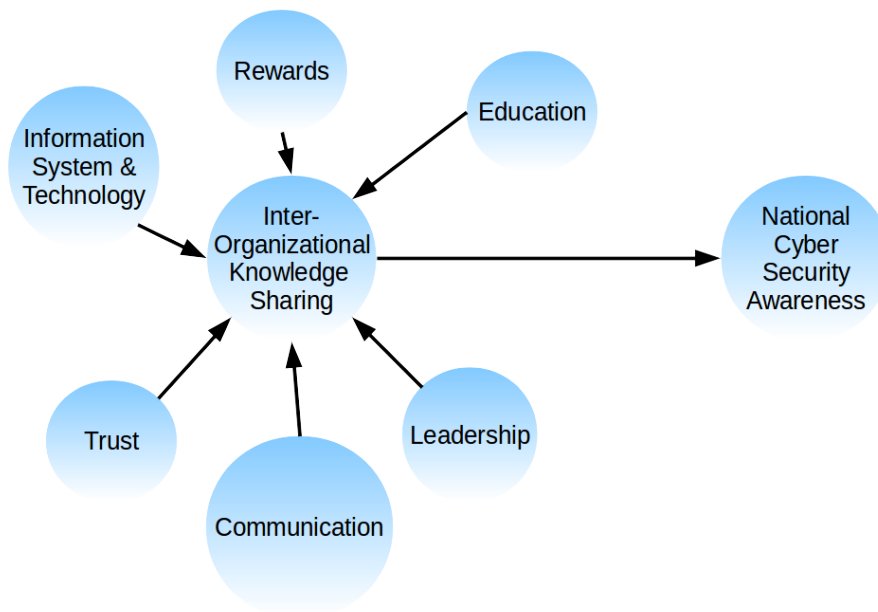


Fig. 2: A model of the proposition

archipelago in the world, Indonesia still have a problem in spreading resources, including educated people evenly. That is why we propose education as an important factor to be considered. On the other hand, our previous research showed that there is a lack in an organization structure in a cyber security related organizations. However, as masculine country, organization structure in Indonesia greatly influenced by the government. As a citizen, we want to contribute in constructing community-based national cyber security awareness in Indonesia. That is why we consider leadership, because it covers people who are able to drive others, in case of cyber security.

V. CONCLUSION

This paper have presented a proposition to study on how inter-organizational collaboration is influential in cyber security awareness behavior. Through an investigation of the knowledge sharing and the leadership, it is expected that more knowledge will be provided on how such are considered as enablers of behavior creation of cyber security awareness within a country setting.

REFERENCES

- [1] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973 – 993, 2014, special Issue on Dependable and Secure Computing The 9th {IEEE} International Conference on Dependable, Autonomic and Secure Computing. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0022000014000178>
- [2] <http://www.surabaya.go.id>, accessed: 2015-10-10.
- [3] <http://www.portal.bandung.go.id>, accessed: 2015-10-10.
- [4] <http://www.jakarta.go.id>, accessed: 2015-10-10.
- [5] R. von Solms and J. van Niekerk, "From information security to cyber security," *Computers & Security*, vol. 38, pp. 97 – 102, 2013, cybercrime in the Digital Economy. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0167404813000801>
- [6] B. Schneier, "Semantic attacks: The third wave of network attacks," <https://www.schneier.com/cryptogram/archives/2000/1015.html#1>, Oct. 2000, accessed: 2015-10-10.
- [7] G. B. White and D. DiCenso, "Information sharing needs for national security," in *System Sciences, 2005. HICSS '05. Proceedings of the 38th Annual Hawaii International Conference on*, Jan 2005, pp. 125c–125c.
- [8] N. A. G. Arachchilage and S. Love, "Security awareness of computer users: A phishing threat avoidance perspective," *Computers in Human Behavior*, vol. 38, pp. 304 – 312, 2014. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0747563214003331>
- [9] G. Saridakis, V. Benson, J.-N. Ezingear, and H. Tennakoon, "Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users," *Technological Forecasting and Social Change*, pp. – , 2015. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0040162515002590>
- [10] P. D. Persadha, A. A. Waskita, and S. Yazid, "Comparative study of cyber security policies among malaysia, australia, indonesia: A responsibility perspective," in *Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec2015), The Fourth International Conference on*, Oct 2015.
- [11] "Indonesia: It community competes in disaster management software development," <http://www.worldbank.org/en/news/feature/2014/08/07/indonesia-it-community-competes-in-disaster-management-competition>, accessed: 2015-10-10.
- [12] "Kawal pemilu 2014," <http://kawalpemilu.org>, accessed: 2015-10-10.

- [13] "Community driven development in indonesia," <http://www.worldbank.org/en/country/indonesia/brief/community-driven-development-in-indonesia>, accessed: 2015-10-10.
- [14] G. B. White, "A grassroots cyber security program to protect the nation," in *System Science (HICSS), 2012 45th Hawaii International Conference on*, Jan 2012, pp. 2330–2337.
- [15] A. Malviya, G. Fink, L. Sego, and B. Endicott-Popovsky, "Situational awareness as a measure of performance in cyber security collaborative work," in *Information Technology: New Generations (ITNG), 2011 Eighth International Conference on*, April 2011, pp. 937–942.
- [16] E. G. Amoroso, "Cyber attacks: awareness," *Network Security*, vol. 2011, no. 1, pp. 10 – 16, 2011. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1353485811700058>
- [17] J. Webb, A. Ahmad, S. B. Maynard, and G. Shanks, "A situation awareness model for information security risk management," *Computers & Security*, vol. 44, pp. 1 – 15, 2014. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0167404814000571>
- [18] U. Franke and J. Brynielsson, "Cyber situational awareness – a systematic review of the literature," *Computers & Security*, vol. 46, pp. 18 – 31, 2014. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0167404814001011>
- [19] R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu, and P. Laplante, "Dimensions of cyber-attacks: Cultural, social, economic, and political," *Technology and Society Magazine, IEEE*, vol. 30, no. 1, pp. 28–38, Spring 2011.
- [20] G. Tadda, "Measuring performance of cyber situation awareness systems," in *Information Fusion, 2008 11th International Conference on*, June 2008, pp. 1–8.
- [21] G. B. White, "The community cyber security maturity model," in *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, Jan 2007, pp. 99–99.
- [22] —, "The community cyber security maturity model," in *Technologies for Homeland Security (HST), 2011 IEEE International Conference on*, Nov 2011, pp. 173–178.
- [23] S. Sajeva, "Encouraging knowledge sharing among employees: How reward matters," *Procedia - Social and Behavioral Sciences*, vol. 156, pp. 130 – 134, 2014, 19th International Scientific Conference "Economics and Management 2014 (ICEM-2014)". [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1877042814059540>
- [24] N. Granado and G. White, "Cyber security and government fusion centers," in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*, Jan 2008, pp. 205–205.
- [25] W. Zhao and G. White, "A collaborative information sharing framework for community cyber security," in *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, Nov 2012, pp. 457–462.
- [26] "The geospatial approach to cybersecurity: Implementing a platform to secure cyber infrastructure and operations," Department of Computer Science, Michigan State University, 380 New York Street Redlands, California, Tech. Rep., June 2015.
- [27] A. Rak, "Information sharing in the cyber age: a key to critical infrastructure protection," *Information Security Technical Report*, vol. 7, no. 2, pp. 50 – 56, 2002. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S136341270202006X>
- [28] Y. Li, Y. Liu, and H. Zhang, "Cross-boundary enterprise security monitoring," in *Computational Problem-Solving (ICCP), 2012 International Conference on*, Oct 2012, pp. 127–136.
- [29] M. Locasto, J. Parekh, A. Keromytis, and S. Stolfo, "Towards collaborative security and p2p intrusion detection," in *Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC*, June 2005, pp. 333–339.
- [30] K. Harrison, J. Rutherford, and G. White, "The honey community: Use of combined organizational data for community protection," in *System Sciences (HICSS), 2015 48th Hawaii International Conference on*, Jan 2015, pp. 2288–2297.
- [31] P. Kirsch, A. Hine, and T. Maybury, "A model for the implementation of industry-wide knowledge sharing to improve risk management practice," *Safety Science*, vol. 80, pp. 66 – 76, 2015. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0925753515001733>
- [32] A. Ismail Al-Alawi, N. Yousif Al-Marzooqi, and Y. Fraidon Mohammed, "Organizational culture and knowledge sharing: critical success factors," *Journal of knowledge management*, vol. 11, no. 2, pp. 22–42, 2007.
- [33] Y.-H. Chen, T.-P. Lin, and D. C. Yen, "How to facilitate inter-organizational knowledge sharing: The impact of trust," *Information & Management*, vol. 51, no. 5, pp. 568 – 578, 2014. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0378720614000408>
- [34] J.-H. Cheng and Y.-C. Fu, "Inter-organizational relationships and knowledge sharing through the relationship and institutional orientations in supply chains," *International Journal of Information Management*, vol. 33, no. 3, pp. 473 – 484, 2013. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0268401213000042>
- [35] V. Shabrina and A. Silvianita, "Factors analysis on knowledge sharing at telkom economic and business school (tebs) telkom university bandung," *Procedia - Social and Behavioral Sciences*, vol. 169, pp. 198 – 206, 2015, the 6th Indonesia International Conference on Innovation, Entrepreneurship, and Small Business (IICIES 2014). [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1877042815003407>
- [36] F. M. Santoro, M. R. Borges, and E. A. Rezende, "Collaboration and knowledge sharing in network organizations," *Expert Systems with Applications*, vol. 31, no. 4, pp. 715 – 727, 2006, computer Supported Cooperative Work in Design and Manufacturing. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S095741740600008X>
- [37] I. Mergel, "Open collaboration in the public sector: The case of social coding on github," *Government Information Quarterly*, pp. –, 2015. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0740624X15300095>
- [38] <https://github.com/>, accessed: 2015-10-10.
- [39] Y. Kim, M. Glassman, and M. S. Williams, "Connecting agents: Engagement and motivation in online collaboration," *Computers in Human Behavior*, vol. 49, pp. 333 – 342, 2015. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0747563215002010>
- [40] "Penerapan smart gateway untuk mendukung komunitas guru belajar (kgb) di bandung, cianjur, dan subang – jawa barat," <http://www.lppm.itb.ac.id/pengabdian/laporanpengabdian/penerapan-smart-gateway-untuk-mendukung-komunitas-guru-belajar-kgb-di-bandung>, accessed: 2015-10-10.
- [41] D. W. Irawanto, "Exploring paternalistic leadership and its application to the indonesian context: a dissertation presented in partial fulfilment of the requirement for the degree of doctor of philosophy in cross-cultural leadership at massey university, palmerston north, new zealand," Ph.D. dissertation, 2011.
- [42] R. Sobandi and N. Sudarmadji, "Knowledge sharing and stakeholder collaboration practice in solo city planning and development: Notes on urban community nurturing processes," *Procedia - Social and Behavioral Sciences*, vol. 184, pp. 161 – 170, 2015, {REFLECTIONS} {ON} CREATIVITY: {PUBLIC} {ENGAGEMENT} {AND} {THE} {MAKING} {OF} {PLACE}. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1877042815033182>
- [43] M. Lundberg and H. Lidelow, "Social motivations for knowledge sharing in construction companies," *Procedia Economics and Finance*, vol. 21, pp. 224 – 230, 2015, 8th Nordic Conference on Construction Economics and Organization. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S2212567115001719>
- [44] R. M. Mayordomo and J. Onrubia, "Work coordination and collaborative knowledge construction in a small group collaborative virtual task," *The Internet and Higher Education*, vol. 25, pp. 96 – 104, 2015. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1096751615000068>
- [45] M. Martínez-Córcoles, F. Gracia, I. Tomás, and J. M. Peiró, "Leadership and employees' perceived safety behaviours in a nuclear power plant: A structural equation model," *Safety Science*, vol. 49, no. 8–9, pp. 1118 –

1129, 2011. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0925753511000725>

- [46] T. Aoyama, H. Naruoka, I. Koshijima, and K. Watanabe, "How management goes wrong? – the human factor lessons learned from a cyber incident handling exercise," *Procedia Manufacturing*, vol. 3, pp. 1082 – 1087, 2015, 6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, {AHFE} 2015. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S2351978915001791>
- [47] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the human aspects of information security questionnaire (hais-q)," *Computers & Security*, vol. 42, pp. 165 – 176, 2014. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S016740481300179X>
- [48] S. R. Kathiravelu, N. N. A. Mansor, T. Ramayah, and N. Idris, "Why organisational culture drives knowledge sharing?" *Procedia - Social and Behavioral Sciences*, vol. 129, pp. 119 – 126, 2014, 2nd International Conference on Innovation, Management and Technology Research. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1877042814028389>



Pratama Dahlian Persadha , was born in Blora, October 14, 1977. Pratama earned a bachelor degree in 2002 from Universitas IP-WIJA Jakarta and master degree in 2005 from University of Indonesia, both concerning on management. However, he attended the various training on network security and cryptography. He is currently a Ph.D student at the faculty of computer science, University of Indonesia concerning on how the cyber security awareness can be built among society. Mr. Persadha is a

chairman and founder of Communication and Information System Security Research Center. He started his career as a staff at Lembaga Sandi Negara – Indonesia. His main task are related to networks security and cryptography. In 2014, he resigned from Lembaga Sandi Negara and establishing Communication and Information System Security Research Center as an IT consultant. He published some IEEE conference paper related to computer network security.



Arya Adhyaksa Waskita , was born on April 24, 1979 in Larat. Arya earned a bachelor degree from Department of Physics University of Indonesia in 2002, and a master degree from Department of Computer Science, Bogor Institute of Agriculture in 2007. He is currently a Ph.D student at the Faculty of Computer Science, University of Indonesia and a researcher at the computational laboratory of National Nuclear Energy Agency since 2003. He published some IEEE conference paper related to computer network security and sensor network. He was awarded the best paper on International Conference on Intelligence and Advances System on 2012.

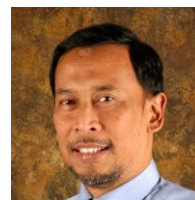
work security and sensor network. He was awarded the best paper on International Conference on Intelligence and Advances System on 2012.



Muhammad Irfan Fadhilla , was born on January 7, 1994. He earned bachelor degree in Information System from the Faculty of Computer Science, University of Indonesia in 2015. He is currently an IT staf of the faculty and joined this research group. His interests are software and system engineering.



Ahmad Kamal , earned bachelor degree in Information System from the Faculty of Computer Science, University of Indonesia in 2015. His interests are software engineering and knowledge management.



Setiadi Yazid Setiadi Yazid earned his bachelor degree from Bandung Institute of Technology in 1978 on electrical engineering, master and Ph.D degree from Queen's university in 1990 on computer and information science and 1995 on computer and electrical engineering. His main research topic is computer and sensor network security.