The Influence Of Security Operation Center Capability And User Awareness On Information Security Performance (Preliminary Study On The Banking Industry In Indonesia)

Toto Alfin Atmojo[1], Idris Gautama So[2], Harjanto Prabowo[3], Sri Bramantoro Abdinagoro[4]

[1,2,3,4] Bina Nusantara University, Anggrek Campus Jl. KebonJeruk Raya No. 27 KebonJeruk Jakarta – Indonesia,

[1]atmojo@gmail.com,[2] igautama@binus.edu, [3] harprabowo@binus.edu, [4] sabdinagoro@binus.edu

ABSTRACT

Information Security is currently becoming a major issue in IT implementation, especially in the banking industry. With the increase of advanced and more sophisticated attacks, and the growth of security incidents and related losses, a better Information Security approach is needed. Empirically, User Awareness has been proven as a component for successful Information Security. Recently, a Security Operation Center (SOC), whose main function is to Identify, Manage, and Remediate attacks, was promoted as a solution to enhance a company's Information Security posture. However, there is no research data that focuses on the change of Information Security through the implementation of SOC. Therefore, research on whether and how SOCs might affect Information Security performance is needed, and that is what differentiates this research from others. As this research evaluates the influence of SOC and User Awareness on overall Information Security Performance.An Exploratory study is conducted, whose units of analysis are banks in Indonesia. A Balanced Scorecard perspective is used as guidance for indicators to measure the impact on Information Security Performance, which will cover technical, financial, and other related indicators. Data gathered from questionnaires are analysed using Partial Least Squares Structural Equation Modeling (PLS-SEM). It was found that both SOC and User Awareness have both apositive and substantialimpact on the performance of Information Security. The end result justifies that investment in SOC will benefit the banking industry specifically, and other industries in general, for improving Information Security Performance.

Keywords

User Awareness, Security Operation Center, Information Security Performance, IT in Banking.

Article Received: 10 August 2020, Revised: 25 October 2020, Accepted: 18 November 2020

Introduction

Information Technology (IT) currently has become an important and strategic part of theorganisation. IT can be a company's Competitive Advantage, which gives it new ways to outperform its competitors (Porter & Millar, 1985). Due to IT ultimately allowingcompanies to cut costs and build discrepancies, it can provide competitive benefits towards the company(Breznik, 2012). Even in the past decade, IT has been linked with its function to create a sustainable competitive advantage for companies (Mata, Fuerst, & Barney, 1995).

Banking is an industry that uses IT intensively, where its adoption of IT is the highest among other industries (Friedrich, Koster, Stroh, & Vollmer, 2013). Among other factors, IT has the most significant impact on Competitive Advantage in Banking through marketing performance (Limakrisna & Yoserizal, 2016). IT holds the critical role of supporting banks' daily operation, and is also one of the main drivers of business transformation, and banking services in the future (PwC Indonesia, 2014). Therefore, banks need to ensure and manage that their IT implementation maintains acceptable performance conditions.

Since IT usage and adoption in banking are significant and critical, it must be ensured that IT implementation is secure. IT in a secure condition is also a part of a key area to be maintained for IT performance measurement (Bianchi, 2001). Banking is defined as critical infrastructure in the United States (DHS, 2014), and has a strategic role to support the implementation of Indonesia's national development (Indonesia Act No. 7 of 1992 and Act No. 8 of 1998). As stated by Bradley, Alvarez, McMillen, & Craig (2016), IT attacks' most common target is the banking sector.Furthermore, for the Internet Banking which considered as one of the bank's channel to its customers, security of customer information is considered as the influencer of customer's behavior (Giri & Wellang, 2016).Banks need to guarantee that all Information Security components (Confidentiality, Integrity, and Availability) exist for the information they have.

One of the causes of the more massive attacks on IT today is the trend of increasingly complex attacks (ISACA, 2015). Over time, attacks arose with a technique, a new type of variant. In fact, some reports informed that incidents of information security are increasing year by year (ISACA, 2015; Ponemon Institute, 2015; PricewaterhouseCoopers, 2016). Meanwhile, existing capacity for blocking and preventing is deemed inadequate to guard against complex, sophisticated, and motivated attacks (MacDonald & Firstbrook, 2016). A Security Operation Center (SOC) is the alternative to protect against advanced and sophisticated attacks faced by companies (MacDonald & Firstbrook, 2016; Muniz, McIntyre, & AlFardan, 2016; Schinagl, Schoon, & Paans, 2015; Zimmerman, 2014).

Even though there is a lot of research, and best practice suggests deployment of SOC, currently there is no empirical research that studies whether and how SOCs impact Information Security performance. Reviewing SOC characteristics, where the main function is to Identify, Manage, and Remediate when an attack occurs, should give more benefit to overall Information Security performance as

its ultimate goal. Therefore, research is needed on how SOCs, along with other variables, affect the performance of information security.

Research background

With the increasingly strategic role of IT for companies, it must be ensured that Information Security is maintained in acceptable conditions. Security is even considered the greatest risk in digital business by Chief Information Officers (Deshpande & Lee, 2016). Furthermore, at a global level, based on the annual report by World Economic Forum's on global risks, information security-related factors are always included in the top 10, along with other major types of risks, such as wars, refugees, and water crises in both the 2015 (World Economic Forum, 2015) and 2016 (World Economic Forum, 2016) reports.

To prevent becoming victims of cyber-attacks, companies also put a significant investment in Information Security. Currently, growth in spending related to information security from 2013 to 2019 increased by 7.9% per year (Elizabeth, Canales, Ruggero, Deshpande, & Pingree, 2016). This figure is well above the all-time IT spending growth of 0.5% per year (Lovelock, Hale, Connell, Atwal, & Graham, 2015). However, some reports mentioned that information security incidents are increasing year by year (ISACA, 2015; Ponemon Institute, 2015; PricewaterhouseCoopers, 2016). Based on the condition above, new security initiatives are needed to handle current Information Security conditions.

It is a challenge for an Information Security team within an organisation to keep users safe while using IT. While almost all IT users in organisation do not have an IT background, attackers are also targeting them as weak targets compared to personnel in the IT department. Research indicates that better user awareness of information security leads to better information security conditions (Bulgurcu, Cavusoglu, & Benbasat, 2010). Hence,companies have to make sure that their users are aware and comply with the information on their security policies.

Since attacks are now more sophisticated and the damage is getting more massive, a Security Operation Center is the key alternative for enhancing Information Security Performance by analyzing and reacting to sophisticated and advanced attacks (MacDonald & Firstbrook, 2016). By building a SOC, a company will have more protection against attacks, will react appropriatelywhen the attack is coming, and will prevent incidents.

Even though there are some recommendations for building a SOC to enhance protection against cyber-attack (Jacobs, Arnab, & Irwin, 2013; Kelley & Moritz, 2006; Kowtha, Nolan, & Daley, 2012; MacDonald &Firstbrook, 2016; Muniz et al., 2016; Schinagl et al., 2015; Zimmerman, 2014), most of them focus on what a SOC is and what its capabilities, the classification and mapping, as well as on how to build a SOC. Since building a SOC is an expensive and difficult task, so the benefit must be justified and proven. Currently, there is no empirical research on the impact of having a SOC for Information Security Performance within a company. Therefore, this research can contribute both to theoretical and practical domains, on how a SOC can impact Information Security Performance, along with other variables.

Research Objectives

There are some objectives of this research as follow:

1. Knowing the role of awareness of IT users, in influencing the conditions of information security in the banking industry in Indonesia.
2. Knowing the role of SOC implementation, in influencing the overall information security conditions in the banking industry in Indonesia.
3. Reviewing current information on security conditions in the banking industry in Indonesia

Research Benefits

This research will enrich the theory of Information Security, where the SOC is part of a variable that contributes to performance. It fills the gap on Information Security research, regarding business and economic aspects of Information Security (Silic & Back, 2014). This research also shows the impact of Information Security on the effectiveness of Information System performance.

In practice, this research also provides benefits both to banking and other industries by creating and implementing information security implementation strategies, as well as IT as a whole, where:

- Information security is one of the priorities for IT implementation and development.
- A Security Operations Center may be considered as one of the initiatives to improve information security efficiency.
- Information Security conditions for the banking industry in Indonesia will be reviewed, especially using a Balanced Scorecard framework as guidance for the indicator.

Literature Review

This research reviews the literature, both from previous research and other qualified materials that cover User Awareness, Security Operation Centers, and Information Security Performance.

User Awareness

IT users, or humans, are often mentioned as the Information Security chain's weakest link chain(Bulgurcu et al., 2010; Mitnick, 2002; Sasse, Brostoff, & Weirich, 2001; Willson, 2016), so this link needs serious attention. Because in many cases, organisations that have built information security with good technology are still frequently exposed to attacks, due to the weak human factor (Schultz, 2005). It has been proven that Information Security which relies solely on technical factors, cannot prevent violations of information security(Parsons, Mccormac, Butavicius, & Ferguson, 2010). Errors and omissions carried out by humans also cause weaknesses in information security (Kraemer, Carayon, & Clem, 2009).

It is defined that user awareness on information security is the understanding, appreciation of needs, objectives and benefits, as well as commitment that will be faced by users. (Albrechtsen, 2007; Choi, Kim, Goo, & Whitmore, 2008;

Siponen, 2000; Torres, Sarriegi, Santos, & Serrano, 2009). From the above explanation, it shows that awareness of information security here must not only be at the level of knowledge, but must be accompanied by actions in accordance with the principles of safe use of IT. Increased awareness of information security will reduce the error rate caused by the users and will maximize the technical, as well as information security procedures from the user'sperspectives(Siponen, 2000). There are some indicators that are used within this research, which are as follows (Bulgurcu et al., 2010; Siponen, 2000; Waly, Tassabehji, & Kamala, 2012):

- User compliance with information security policy (UA1)
- User compliance with safe computer usage procedures (UA2)
- Data protection at the user level (UA3)
- Overall user awareness of information security and its negative implications (UA4)

SOC Capability

Information security within a company is supported by one of the important components which is Security Operation Center (SOC). More specifically, a Cyber SOC is a set of activities consisting of cyberspace safeguards, by monitoring and analyzing threats and incidents, as well as proactively and responsively managing incidents (Kowtha et al., 2012). Zimmerman (2014) sees SOC through what SOC does, which performs the functions of Computer Network Defense (CND), which is a technique for defending unwarranted computer network operation, including tracking, identification, reaction review and enhancement activities.

In overall concept, having a SOC aims to have a real-time view the network conditions or the security status of an organisation, ensuring that the system is not negatively impacted and that it has the ability to perform actions aligned with consistent protocols and processes when something happens, as well as ensuring that someone monitors the existing facilities at all times (Nathans, 2015). In detail, there are several purposes of a SOC as revealed by (Michail, 2015) and (Kelley & Moritz, 2006). The first is to find out what happens to the entire IT infrastructure (especially related to security). Next, is to reduce the risk and the occurrence of downtime (dead system), because the security conditions have improved with the SOC. The next goal is to control and prevent threats, in addition to continuously improving defense mechanisms, as well as working with outsiders to stay current. The SOC also aims to reduce administrative costs, as data is collected, processed, and analysed automatically to then become the basis of decisions, thereby reducing the cost of human resources.

To see the effectiveness of the SOC, it is necessary to look at the extent of the capabilities and performance. Jacobs et al., (2013) and Muniz et al., (2016) provides comprehensive information on aspects that every SOC must have. This study will detail the capability of each aspect of a SOC, which is divided into 3 (three) dimensions as follows:

- Technology:
  - Log Management (SOC1)
  - Threat Identification (SOC2)
  - Dedicated Security Personnel/Team has the capability to manage threats and incidents (SOC3)
  - Regular training for security personnel to stay updated on current threats (SOC4)
- Process
  - Threat & Incident Management (SOC5)
  - Reporting (SOC6)

The Capability Maturity Model has tools that can be used to measure the effectiveness of the management process (Muniz et al., 2016). The model has 6 (Six) maturity levels that can be mapped to current processes or conditions within an organisation:

0. Non-Existent
1. Initial/AdHoc
2. Repeatable but Intuitive
3. Defined Process
4. Managed and Measurable
5. Optimized

This research uses Control Objectives for Information and related Technology (COBIT) Maturity Model (MM), which was developed by ISACA. Each aspect of the SOC above will be reviewed and mapped on its capability using COBIT MM, and its effect on overall Information Security Performance will be analysed.

Information Security Performance

Information security must be ensuredin order to be maintained at the level that the company requires.Companies should be able to evaluate their information security efficiency in order to take the best actions that are consistent with the company's information security needs (Bernik&Prislan, 2016).Furthermore, since the information technology budget is not minimal, companies often want to see what advantages these expenditures will result in(Huang, Lee, & Kao, 2015).

By measuring the performance of information security, companies can see how well their needs for security have been met (Bernik & Prislan, 2016). In some cases, the measurement of information security performance is even a necessity, such as for regulatory compliance purposes (Chew, Swanson, Stine, Bartol, Brown, & Robinson, 2008). Therefore, the measurement of information security performance becomes important to the overall corporate information security strategy.

There is some literature that specifically addresses the performance or effectiveness of information securitythrough various approaches. Choi, Kim, & Goo (2006)state that an organisation's success in information security is determined by its dedication and response to information security management.Similarly, Kankanhalli, Teo, Tan, & Wei (2003) stated that a strong or successful performance in information security is considered as the ability in protectingorganisational information assets against access breaches or intentional misuse.

When security performance is evaluated solely on the basis of technical aspects, challenges need to be addressed. First, because sometimes the benefit is intangible, like starting security awareness program, or creating a security awareness poster. The other reason is, sometimes the benefit of having a security initiative is unquantifiable, such as implementing a firewall while the number of potential attacks is unknown. Meanwhile, management needs more

quantifiable justification (such as financial justification) before an investment for information security is initiated.

Besides the technical approaches above, another study was conducted by Huang et al., (2015) and Herath, Herath, & Bremser, (2010), that included business aspects of information security performance by using Balanced Scorecard (BSC) framework. In addition, it is not about a study of defense efficiency details focused on financial considerations alone. The information security performance was viewed using 4 BSC perspectives, namely: Financial, Customer, Internal Process, and Learning & Growth. These four perspectives were then associated with relevant information security success metrics, resulting in a consistent estimation for the overall organisation.

The BSC framework is used as guidance for indicators in this research, since it gives a more comprehensive approach by adding non-financial performance, and it also accommodates the intangible value of information on security performance, such as user awareness. Below are the BSC indicators used to measure information security performance for this research (Herath et al., 2010; Huang et al., 2015; Straub, 1990), which are divided into 4 (four) dimensions:

- Financial Perspective:
  - Financial damage caused by information security incident that can be avoided (ISP1)
  - Financial benefits of implementing Information Security (ISP2)
- Customer Perspective:
  - Information Security Implementation meets stakeholder's expectation (ISP3)
- Internal Process Perspective:
  - Information Security Performance at the organisation level (ISP4)
  - Information security implementation is adequate for reducing vulnerability and threats (ISP5)
- Learning & Growth Perspective:
  - Ability to prevent and deal with information disaster (ISP6)

Materials And Methods

Theoretical Framework

The banking industry has a strategic role to support the implementation of Indonesia's national development. Banks are finding ways to improve their company's performance to meet expectations and win over the competition. IT is known as an option that can bring a competitive advantage to a company (Bharadwaj, 2000; Dehning & Stratopoulos, 2003; Porter & Millar, 1985). Meanwhile, banking is an industry that is implementing IT on a large scale, both for strategic and operational purposes. Therefore, banks need to monitor and maintain their IT performance at an acceptable level. To ensure IT performance at an acceptable level, banks need to monitor various aspects that form their IT Performance.

The performance of Information Security is one aspect that has to be ensured. IT Performance will never be achieved without the existence of Confidentiality, Integrity, and Availability. Maintaining Information Security performance is more challenging, because challenges come from both sides: ITusers and attackers. Users are demanding that the ease of use and functionality of technology remain the same when implementing security initiatives, which is very challenging. Meanwhile, attacks are becoming more sophisticated and the damage is getting worse.

By implementing SOC, banks are serious about improving Information Security performance. SOC is defined as a way to handle traditional attacks (Viruses, Internet misuse, SPAM, illegal website access) up to more sophisticated attacks (Advanced Persistent Threats, targeted attacks, etc). Looking into some functions and the usage of SOC, it can be assumed that SOCs can improve Information Security Performance, even if an empirical study is still needed.

User Awareness is a variable that usually exists when discussing important variables that form Information Security (Choi et al., 2008; Torres et al., 2009). Banks must ensure that user awareness on information security is maintained, to keep Information Security Performance at an acceptable level. In this study, the role of SOCs on moderating User Awareness to influence overall Information Security Performance is tested.

The above framework is developing a research model that can be used to achieve the research objectives. The theoretical research framework that is based on this model will describe the effect of each variable.

Hypotheses

Based on the above literature review and theoretical framework, the research hypotheses are as follow:

Hypothesis 1: User awareness of Information Security has a significant influence on Information Security Performance.

Hypothesis 2: SOC capability has a significant influence on information security performance.

Variable Operation

This study consists of 3 (three) variables, with 15 (fifteen) indicators to be reviewed, as follows:

1. User Awareness as an exogenous variable;
2. Capability of SOCs as an exogenous variable;
3. Information Security Performance as an endogenous variable

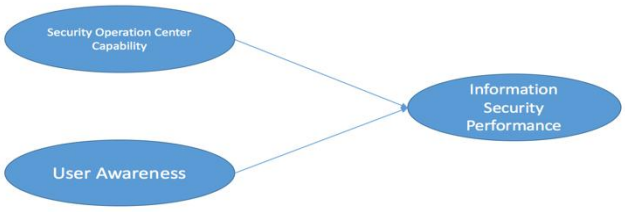

Figure 1: Research Model

Sampling Selection Technique

The population for this research is the Commercial Bank in Indonesia. Based on data from Indonesia banking, there are 120 commercial banks (Bank Umum) and Sharia Bank (Bank Syariah) in Indonesia (Indonesia, n.d.). Non-probability sampling with purposive sampling was used to

choose a subject from the sample that was available. This type of purposeful sampling used is judgement sampling, where subjects are chosen who are in the best position to provide the information required. This study was conducted by contacting Chief Information Office (CIO) or Senior IT position (IT Director, IT Manager, Head of IT Security, etc.) from each bank, to answer some questions on the questionnaire. The questionnaire was sent through email to the respective person for each bank.

Analysis Structure and Hypotheses Testing

During the survey, all indicators of each variable were provided to the respondents. The value of each indicator was measured using a Likert scale.Hypotheses testing was conducted using the Structural Equation Model based on Partial Least Square (PLS-SEM). PLS-SEM was used since this research is developing a model by focusing on dependent variable variance (Hair, Hult, Ringle,& Sarstedt, 2014). Results from the PLS-SEM will verify the correlation and influence of User Awareness and SOC Capability to Information Security Performance.
Validity testing of all indicators resulted in loading value above 0.7 for all indicators. Meanwhile, reliability testing of all indicators resulted in composite reliability above 0.7 for all indicators. This means that all indicators are valid and reliable:

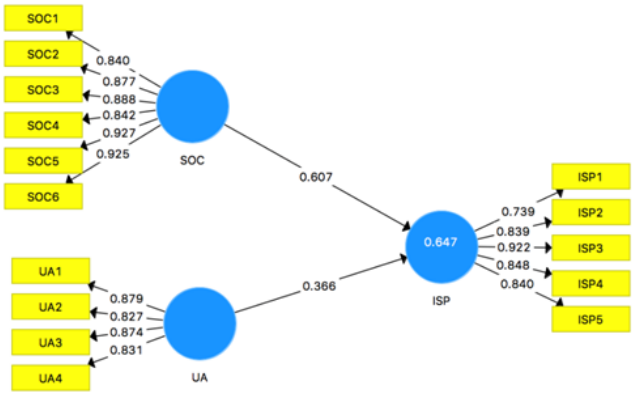

Figure 2: Construct Model

Results And Discussions

According to the 10 times rule Hair et al., (2014) state that the minimum sample size for the model should be 10 times the maximum number of arrows pointedtoward the latent variable.Linked to this analysis, if there are two cumulative arrows pointed at a latent component, then the minimum sample size is 20.The sample size for this study was 37 respondents from different banks in Indonesia.Therefore, the number of samplesof this research is complying to the minimum sample size required by SEM-PLS to run.
Banks that participate on this research consist of 4 state-owned banks (from total 4 banks), 14 foreign exchanged banks(from total 35 banks), 6 non-foreign exchange banks (from total 31 banks), 7 regional banks (from total 27 banks) and 6 joint-venture banks (from total 14 banks).Among all respondents, 87% are manager or section head and there are 6% from staff position. Profile of respondents are 45% from IT Security division, 45% from IT Division and the rest are mix (ATM team, Operation, etc).
Statistical calculation using PLS-SEM was used to discover the influence of the Independent Variable on the Dependent Variable. To test whether the Independent Variable was partially having a significant influence on the Dependent Variable, a t-test was used. This research used a 95% confident level, which means that the alpha value was 5% and the t table was 1.96. The t-test for UA -> ISP was 2.83, which is also above t table value, meaning that User Awareness has a positive and significant influence on Information Security Performance. This result is aligned with research conducted by Casaca (2014), where user awareness is positively related to the effectiveness of information security management in SME (Small Medium Enterprise).
Meanwhile, the t-test for SOC -> ISP was 4.56, which is far above the t table value, meaning that SOC Capability has bothpositive and substantial influence on Information Security Performance.The model also suggests that SOC has a more significant impact on the efficiency of information security compared with user awareness.From Figure 2, the structural equation can be constructed as follow: ISP = 0.607*SOC + 0.366*UA + e. Since the R Adjusted value is 0.622, it can be concluded that 62.2% of ISP Variants can be explained by some changes in the SOC and UA variables, while the other 37.8% is caused by other factors outside the model.
From the statistical calculation above, the results for the Hypotheses testing are as follows. Hypotheses 1, where "User awareness on Information Security has a significant influence on Information Security Performance" is accepted. Meanwhile, hypothesis 2, where "SOC capability has significant influence on information security performance" is accepted as well.

Conclusion

The banking industry is using IT as a key initiative, both for enabling business and also as one of the main tools for competitive advantage. Furthermore, since banking is a highly sensitive industry where a security breach could damage its reputation and customer trust, the need for information security protection is high. Banks need to ensure that their Information Security performance is at an acceptable level. Using a Balanced Scorecard approach, Information Security performance will be seen not only from a financial perspective but also through a more holistic approach where non-financial and technical perspectives are also covered. The BSC framework can be used as guidance for measuring indicators of Information Security Performance.
User awarenesson the confidentiality of information is an important aspect in retaining secure information due to being a significant factor in information security, which is aligned with previous studies. Meanwhile, building a SOC is one option for a company to enhance its information security performance. By having aSOC, banks will have the major functions to Identify, Manage, and Remediate when an attack is occurring and will be able to minimize damage by implementing and running the Security Operation Center.

As well as incorporating User Awareness, banks will have the ability to enhance their performance on Information Security.

This research is analyzing the influence of two independent variables (SOC and user awareness) that has 62.2% changes over the independent variable (information security performance). There is still chance to look another significant variable that might also influence ISP, and put into the model like Technology, Governance (Casaca, 2014) or Management Support (Choi et al., 2008; Kankanhalli et al., 2003). The study can also be improved by enlarging the number of respondents, to get a morevalid result and improve its validity.

References

[1] Albrechtsen, E. (2007). A qualitative study of users' view on information security. Computers and Security, 26(4), 276–289. Retrieved from https://doi.org/10.1016/j.cose.2006.11.004

[2] Bernik, I., & Prislan, K. (2016). Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation.PLoS ONE, 11(9), 1–34. Retrieved from https://doi.org/10.1371/journal.pone.0163050

[3] Bharadwaj, A. S. (2000). A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation.MIS Quarterly, 24(1), 169–196. Retrieved from https://doi.org/10.2307/3250983

[4] Bianchi, A. J. (2001). Management Indicators Model To Evaluate Performance of IT Organizations. Management of Engineering and Technology, 1(28).

[5] Bradley, N., Alvarez, M., McMillen, D., & Craig, S. (2016). 2016 Cyber Security Intelligence Index. Retrieved from http://www-01.ibm.com/common/ssi/cgibin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF

[6] Breznik, L. (2012). Can Information technology be a source of competitive advantage ? Economic and Business Review, 14(3), 251–269.

[7] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523–548. Retrieved from https://doi.org/10.1093/bja/aeq366

[8] Casaca, J. A. (2014). Determinants of the information security effectiveness in small and medium sized enterprises. Proceedings in EIIC-The 3rd Electronic International Interdisciplinary Conference, 3(1), 495–500. Retrieved from http://www.eiic.cz/archive/?vid=1&aid=2&kid=20301-51

[9] Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2008). Performance measurement guide for information security. NIST Special Publication, 800–55(July), 80.

[10] Choi, N., Kim, D., & Goo, J. (2006). Managerial information security awareness' impact on an organization's information security performance. In Americas Conference on Information Systems (AMCIS), 406.

[11] Choi, N., Kim, D., Goo, J., & Whitmore, A. (2008). Knowing is doing an empirical validation of the relationship between managerial information security awareness and action. Information Management & Computer Security, 16(5), 484–501. Retrieved from https://doi.org/10.1108/09685220810920558

[12] Dehning, B., & Stratopoulos, T. (2003). Determinants of a sustainable competitive advantage due to an IT-enabled strategy. Journal of Strategic Information Systems, 12(1), 7–28. Retrieved from https://doi.org/10.1016/S0963-8687(02)00035-5

[13] Deshpande, S., & Lee, P.L. (2016). 2016 CIO Agenda: A Southeast Asia Perspective. Retrieved from

https://www.gartner.com/doc/3218918/-cio-agenda-southeast-asia

[14] DHS. (2014). Critical Infrastructure Sectors. Retrieved June 19, 2016, from https://www.dhs.gov/critical-infrastructure-sectors

[15] Elizabeth, K., Canales, C., Ruggero, C., Deshpande, S., & Pingree, L. (2016). Forecast Analysis : Information Security , Worldwide , 2Q15 Update. Retrieved from https://www.gartner.com/doc/3126418/forecast-analysis-information-security-worldwide

[16] Friedrich, R., Koster, A., Stroh, S., & Vollmer, C. (2013). The 2012 Industry Digitization Index. Retrieved from http://www.booz.com/media/file/BoozCo_The-2012-Industry-Digitzation-Index.pdf

[17] Giri, R. R. W., & Wellang, K. M. (2016). Impact of website design, trust, and internet skill on the behaviour use of site internet banking in Bandung Raya: A modification of the utaut model. Pertanika Journal of Social Sciences and Humanities, 24(S), 35–50.

[18] Herath, T., Herath, H., & Bremser, W. G. (2010). Balanced scorecard implementation of security strategies: A framework for it security performance management. Information Systems Management, 27(1), 72–81. Retrieved from https://doi.org/10.1080/10580530903455247

[19] Huang, S.M., Lee, C.L., & Kao, A.C. (2015). Balancing performance measures for information security management: A balanced scorecard framework. Industrial Management & Data Systems, 106(2), 242–255. Retrieved from http://www.ijcaonline.org/archives/volume141/number8/rosmiati-2016-ijca-907930.pdf

[20] Indonesia, B. (n.d.). Daftar Nama Kantor Pusat Bank di Indonesia. Retrieved July 7, 2017, from http://www.bi.go.id/id/publikasi/laporan-keuangan/alamat-bank/umum/Default.aspx

[21] ISACA. (2015). State of Cybersecurity : Implications for 2015. Retrieved from https://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf

[22] Jacobs, P., Arnab, A., & Irwin, B. (2013). Classification of security operation centers. 2013 Information Security for South Africa, 1-7. Retrieved from https://doi.org/10.1109/ISSA.2013.6641054

[23] Hair, J. F., Hult, G. T. M., Ringle, C. M.,& Sarstedt, M. (2014). A primer on partial least squares structural equation modeling (PLS-SEM). California: SAGE Publications.

[24] Kankanhalli, A., Teo, H.H., Tan, B. C. Y., & Wei, K.K. (2003). An integrative study of information systems security effectiveness. International Journal of Information Management, 23(2), 139–154. Retrieved from https://doi.org/10.1016/S0268-4012(02)00105-6

[25] Kelley, D., & Moritz, R. (2006). Best practices for building a security operations center. Information Systems Security, 14(6), 27–32. Retrieved from https://doi.org/10.1201/1086.1065898X/45782.14.6.20060101/91856.6

[26] Kowtha, S., Nolan, L. A., & Daley, R. A. (2012). Cyber security operations center characterization model and analysis. 2012 IEEE Conference on Technologies for Homeland Security (HST), 470–475. Retrieved from https://doi.org/10.1109/THS.2012.6459894

[27] Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers and Security, 28(7), 509–520. Retrieved from https://doi.org/10.1016/j.cose.2009.04.006

[28] Limakrisna, N., & Yoserizal, S. (2016). Determinants of marketing performance: Empirical study at National Commercial Bank in Jakarta Indonesia. SpringerPlus,

5(1), 1693. Retrieved from https://doi.org/10.1186/s40064-016-3362-3

[29] Lovelock, J.D., Hale, K., Connell, A. O., Atwal, R., & Graham, C. (2015). Forecast Alert: IT Spending, Worldwide, 3Q16 Update. Retrieved from https://www.gartner.com/doc/3471552/forecast-alert-it-spending-worldwide

[30] MacDonald, N., & Firstbrook, P. (2016). Designing an Adaptive Security Architecture for Protection From Advanced Attacks, 1–8. Retrieved from https://www.gartner.com/doc/2665515/designing-adaptive-security-architecture-protection

[31] Mata, F. J., Fuerst, W. L., & Barney, J. B. (1995). Information technology and sustained competitive advantage: A resource-based analysis. MIS Quarterly, 19(4), 487–505. Retrieved from https://doi.org/10.2307/249630

[32] Michail, A. (2015). Security Operations Centers: A Business Perspective. Utrecht University. Retrieved from https://dspace.library.uu.nl/bitstream/handle/1874/315912/Security%20Operations%20Centers%20%20A%20Business%20Perspective.pdf;sequence=2

[33] Mitnick, K. (2002). The art of deception. Indianapolis: John Wiley, Inc.

[34] Muniz, J., McIntyre, G., & AlFardan, N. (2016). Security operations center: Building, operating, and maintaining your SOC. Indianapolis: Cisco Press.

[35] Nathans, D. (2015). Designing and building security operations center. Syngress.

[36] Parsons, K., Mccormac, A., Butavicius, M., & Ferguson, L. (2010). Human Factors and Information Security : Individual , Culture and Security Environment. Retrieved from https://pdfs.semanticscholar.org/07f8/c87e6bb79ffb3ad846168a641dc750cb85e8.pdf

[37] Ponemon Institute. (2015). 2015 Cost of Cyber Crime Study: Global. Ponemon Institute Research Report. Retrieved from http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/index.html?jumpid=va_fwvpqe387s

[38] Porter, M. E., & Millar, V. E. (1985). How information gives you competitive advantage. Harvard Buiness Review, 63(4), 149-160. Retrieved from https://doi.org/10.1038/bdj.2007.481

[39] PricewaterhouseCoopers. (2016). The Global State of Information Security Survey 2016. Retrieved from https://doi.org/10.1038/483531a

[40] PwC Indonesia. (2014). Indonesian Banking Survey 2015. Retrieved from https://www.pwc.com/id/en/publications/assets/banking-survey-2015.pdf

[41] Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the “weakest link” - A human/computer interaction approach to usable and effective security. BT Technology Journal, 19(3), 122–131. Retrieved from https://doi.org/10.1023/A:1011902718709

[42] Schinagl, S., Schoon, K., & Paans, R. (2015). A framework for designing a security operations centre (SOC). Proceedings of the Hawaii International Conference on System Sciences (HICSS), 2253–2262. Retrieved from https://doi.org/10.1109/HICSS.2015.270

[43] Schultz, E. (2005). The human factor in security. Computers and Security, 24(6), 425–426. Retrieved from https://doi.org/10.1016/j.cose.2005.07.002

[44] Silic, M., & Back, A. (2014). Information security: Critical review and future directions for research. Information Management & Computer Security, 22(3), 279–308. Retrieved from https://doi.org/10.1108/IMCS-05-2013-0041

[45] Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 31–41. Retrieved from https://doi.org/10.1108/09685220010371394

[46] Straub, D. (1990). Effective IS security: An empirical study. Information Systems Research, 1(3), 255–276.

[47] Torres, J. M., Sarriegi, J. M., Santos, J., & Serrano, N. (2009). Managing information systems security: Critical success factors and indicators to measure effectiveness, International Conference on Information Security, 530–545.Retrieved fromhttps://doi.org/10.1007/11836810_38

[48] Waly, N., Tassabehji, R., & Kamala, M. (2012). Improving organisational information security management: The impact of training and awareness. 2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems, 1270–1275. Retrieved from https://doi.org/10.1109/HPCC.2012.187

[49] Willson, D., & Dalziel, H. (2016). Cyber security awareness for CEOS and management. Waltham, MA: Syngress.

[50] World Economic Forum. (2015). Global Risks 2015, 10th Edition. Retrieved from www.weforum.org/risks

[51] World Economic Forum. (2016). The Global Risks Report 2016, 11th Edition. Retrieved from http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf

[52] Zimmerman, C. (2014). Ten Strategies of a World-Class Cybersecurity Operations Center. MITRE Corporation report release. Retrieved from https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf