Improving Information Security Performance: The Role of Management Support and Security Operation Center

T. A. Atmojo, H. Prabowo, I. G. So, S. B. Abdinagoro

***Abstract**: The implementation of Information Technology (IT) in any aspects of business has change the landscape of business. Specifically, IT has made significant and major changes in banking industry, especially on the way people do business with bank. Beside as business enabler, IT now become a major tool for bank to win the competition. With the strategic role of IT in banking industry, there is a risk from security point of view. The new sophisticated and advanced kind of attack drive to higher impact for banks. Beside direct loss caused by successful attack, there is also loss caused by image damage and sanction from regulatory. With many initiatives can be done to improve Information Security condition, banking need to prioritize the initiative that has most significant impact. Management support on information security is cited by many literatures as basic requirement for improving Information Security condition. Security Operation Center also proposed as initiatives to enhance the capability of detection and response to attack. This research tries to empirically find out the impact of Management Support to information security performance and the role of Security Operation Center on mediating both variables. Data are gathered from banks in Indonesia using survey methodology through questionnaire answered by qualified respondents. The sample design used is a probability sample with disproportionate stratified random sampling and analyzed using Structural Equation Modeling - Partial Least Square. This paper shows that management support has significant impact on improving Information Security condition in banking industry. It also concludes that SOC has complimentary mediation of relationship between management support and information security performance. Practically, result of this research can be foundation for company that wants to focus on factors that significantly impact security performance, while theoretically confirmed previous studies on the role of management support.*

Keywords: **Banking Industry, Information Security Performance,** ***Management Support, Security Operation Center, SEM-PLS.***

Revised Manuscript Received on 30 July 2019.
* Correspondence Author

T. A. Atmojo, Department of Information System Management, Bina Nusantara University. Indonesia.

Harjanto Prabowo*, Professor, Department of Information System Management, Bina Nusantara University. Indonesia.

Idris Gautama So, Associate Professor, Department of Information System Management, Bina Nusantara University.

Sri Bramantoro Abdinagoro, faculty member of Binus Business School in Jakarta, Indonesia.

I. INTRODUCTION

It is no doubt that Information Technology (IT) currently plays important role in many organization and business. IT has changed the way people doing business into cheaper, better and faster ways.

In Banking, IT also plays a significant role for daily operation and also the ways it serves customer. With the rise of Internet and mobile phone, bank customer now use IT (using both channel) to do interaction with bank more than direct meeting with bank personnel [1]. Furthermore, among other industries, banking is the top position on digital adoption index [2]. It is proven that now banking are moving into a more digital institution. Besides the benefit of implementing IT, there are many risks that faced by banking industry, and one of it is security risk. It is fact that security incident are increasing over the years, with more advanced of attack vectors and also higher impact to the company [3], [4], [5]. According to IBM X-Force research, banking is categorized as most targeted sector for cyber-attack [6]. Meanwhile, there are many solutions to enhance the information security that can be chosen. It is important for banking industry to prioritize the solution that has significant impact on information security performance. Implementation of Information Security initiative and program receive support from all stakeholder within the company, including management level. Management support on information security is the critical success factor of information security performance, that most cited by literature of information security management [7]. Support from management level is also needed because they are the target of cyber-attack, since they hold valuable information within the company [8], [9].The higher awareness and support from management level to information security, the more efficient company performance related to IT security[10]. When cyber-attack are more advanced and sophisticated, and causing both financial and non-financial loss, current solutions to block and prevent the attacks are considered not sufficient [11]. Company need new way to have better detection on advanced and sophisticated cyber-attack, and therefore can create better protection mechanism. Security Operation Center (SOC) is an initiative that can be developed by company to protect against above kind of cyber-attack [11]–[13].

In developing SOC, management support also holds very important role. SOC must has support from management even before it is developed [13].

Management support is needed, not just because developing SOC need big investment, but also SOC must able to do coordination with other division even outside IT department [14]. On the other hands, sponsorship and support from executive level is the most important things for SOC to operate and has good capability [12].

There is a need for empirical evidence, on how management support and SOC influence information security performance. It also needed to find out that the significance of influence, if any. In this research, SOC is considered as mediator of relationship between management support and information security performance. We need to find out what kind of mediation that SOC has on management support and information security performance relationship.

II. LITERATURE REVIEW

A. *Information Security Performance*

Information security is about protecting the Confidentiality, Integrity and Availability of information [15]. **Confidentiality** means that the information is can be accessed only by authorized party. **Integrity** is the condition where an entity (information or IT) is trustworthy, meaning that it is not changed by someone not authorized. While **Availability** is ensuring that IT and information is available to be accessed by authorized party when needed. Information Security Performance is about to ensure that three aspects of information security above at acceptable condition, within the company.

Company must have objective and goal of information security performance, and assess their current condition whether it is aligned with the goal [16]. Assessing current condition will determine the gap with information security objective (if any) and guide us to fill the gap. In addition, assessing information security performance is needed since budget for information security is big, and management need to see the benefits that are derived from these investments [17]. In some cases, it is a mandatory for company to do assessment of information security performance, due to regulatory compliance [18].

To measure information security performance, there are some approaches that can be used. It is can be seen as the ability of organization to protect its information assets against access violation or deliberate misuse [19]. It is also influenced by commitment to and action management of information security [10].

Another way to measure the performance of information security is by using Balanced Scorecards (BSC) approach [17], [20]. BSC is not only a review of information on security performance based only on financial aspects or technical aspects, but more comprehensive. Using BSC, information security performance was assessed through 4 BSC perspectives, namely: Financial, Customer, Internal Process, and Learning & Growth. The four perspectives in the BSC were then linked to various performance indicators of information security, resulting in a balanced calculation for the organization as a whole [17], [20], [21].

B. *Management Support on Information Security*

Management support within a company for information security also plays an important role in information security performance within the company. Management support is defined as support and commitment from management of company, for events, initiatives and other related needs to improve the condition of information security within the company. This is how management (directors and managers) understand and support the impact of information security for businesses and their stakeholders [7]

The greater the support from the top level in management, resulting more effective the information security on the company [22]. Therefore, organizational support (in this case management) positively affects the performance of information security [23]. Furthermore, support from senior management is the most important factor for the successful information security risk management program of a company [24]. This confirms that information security is not only the responsibility of the information security division or IT division, but it should be part of a strategy at the management level. Aligned with above research, the awareness from management related to information security also increase. According to research by The Economist Intelligence Unit, cyber security is the highest concern of bank while focusing its digital investment [25]. Especially in banking industry, where the evolution into more digital channel are being deployed, security is a foundation for the business where management is really concern.

C. *Security Operation Center*

Security Operation Center (SOC) is defined as centralized security organization, that helps company to identify, manage and remediated against security attack [26]. Furthermore, SOC is 'a team' that consist of security analyst formed to detect, analyzed, response, report and prevent of security incident [13]. SOC also an important component of company that want to comply with regulatory compliance and also comply with threat management [26].

The ultimate goal of SOC is: Security [14]. In more detail, the final goals of SOC is to improve information security performance of a company, by detect and response of threat before has impact to the business [26]. Specifically, there are four goals that want to achieved by developing SOC within a company: finding security event, minimize risk of downtime caused by security event, control and prevent threat and at the end doing forensic when incident happened [27], [28]. In summary, SOC is developed because its capability to detect, prevent, react and remediate any security incident, while also assist the company to comply with regulatory compliance [26].

To be defined as SOC, and organizations must have at least ten characteristics [26]. First is **collecting log**, while also **store and archive log**. Next is the ability to **analyze log** that has been collected. SOC must also able to **analyzed different kind of devices** and doing **monitoring of security event**. Furthermore, SOC must be able to do **correlation between events**, **identifying threats** and **react to those threats**. At the end, SOC must be able to do **incident management** and **reporting**.

III. METHODOLOGY

A. *Research Framework*

Management support plays very important role on information security performance within an organization.

There is need of support and commitment from senior management to information security management [29]. The more awareness and support from management to information security, will impact on more efficient performance of company on IT Security [10]. Awareness from management level on information security also impact and has positive relationship on action to information security [30]. Organization with support from top level management is proven to more focus on prevention, compared with management with lower top management support [19].

Meanwhile, there is growth of types, numbers and complexity of attack on IT, causing massive loss. The more company use IT strategically like in Banking, causing more significant loss. To overcome the growth of attack, development of Security Operation Center is one of the alternative [11], [12], [14], [31]. SOC with good capability is proven to enhance information security performance by the ability to detect attack quickly, therefore company can react to the attack faster [26], [31].

Based on above facts, there is need to find out empirically on how management support can improve information security performance of a company. It also important to knows that how capability of SOC can mediate the relationship between management support and information security performance. Below is the model of this research:

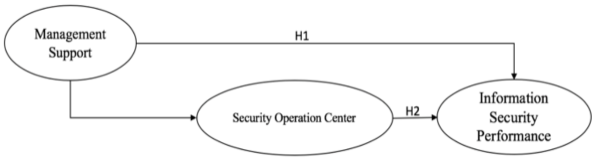


Figure 1. Research Model

B. *Variable Operation*

Information security performance are defined as the achievement of the state of information security in the company, in accordance with the targets to be achieved. This variable uses the perspective of the IT Balanced Scorecard as a measurement reference defined in four dimensions, namely financial, customer, internal processes and growth and learning. This variable consists of ten indicators measured using the Ordinal scale. The indicators for this variable are:

- **ISP1.** The company is able to avoid financial losses caused by information security incidents [17], [21].
- **ISP2.** The financial benefits of implementing information security in a company exceed the costs incurred [20].
- **ISP3.** Accuracy of IT-based transactions can be guaranteed [17].
- **ISP4.** E-commerce bank transactions can be trusted / relied upon [17].
- **ISP5.** Customers are satisfied with the company's IT services [17].
- **ISP6.** Implementation of information security in company in accordance with stakeholder expectations [20].
- **ISP7.** Conditions for implementing information security in banks at a good level [17].
- **ISP8.** The implementation of information security is sufficient to reduce weaknesses and security threats [20].
- **ISP9.** Ability to prevent and deal with information related disasters [17].
- **ISP10.** There is training and education regarding adequate information security for IT users [17].

Security Operation Center is defined as the function that able to identify, manage and correct attacks that arise. This variable consists of six indicators. The entire indicator is measured using an ordinal scale, to see the extent of its capability. The measurement parameters of each indicator use a measurement benchmark based on the Capability Maturity Model. The indicators of this variable are [12], [26]:

- **SOC1.** Log management function.
- **SOC2.** Ability to identify attacks.
- **SOC3.** Availability of IT security personnel who have the ability to handle attacks & incidents.
- **SOC4.** There is periodic training for IT security personnel to be updated for the latest attack information
- **SOC5.** The company's ability to manage management against attacks and incidents
- **SOC6.** Ability to make reports regarding attacks and incidents

Management support for information security is defined as Management's support and commitment, to activities, initiatives and other needs to improve information security of the company. This variable consists of four indicators, which are measured using an ordinal scale. The forms of support seen in this variable range from participation in information security activities, policy formation to support for information security budgets. The indicators for this variable are:

- **MS1.** Establishment of Information Security Policies and Procedures [7], [30].
- **MS2.** Approval and support for Information Security training [7], [30].
- **MS3.** Approval and support of Information Security functions or work units [30].
- **MS4.** Investment support for Information Security [32].

C. *Hypotheses Development*

Based on the previous explanation, this study aims to determine the extent to which management support affects the performance of information security. Therefore, the information security performance variable is the latest endogenous variable.

Information security performance are influenced by various aspects, one of which is management support for information security. The existence of the SOC is a new aspect, which is the novelty of this research, with the capability of the SOC taken into account in mediating the influence of the relationship between management support for conditions of information security.

Based on the background and objectives of the above research, it is necessary to formulate a hypothesis that is in accordance with the framework of the previous thinking. The hypothesis is a temporary statement, which can be tested, which predicts what we expect to find in the empirical data that we have [33].

This study uses the deductive reasoning method, with research starting from a more general phenomenon, namely information security performance, then more specific aspects are examined, namely related to management support and the capability of SOC as a mediator. Based on research model in Figure 1 above, below are the hypotheses of this research:

- **H1.** Management support is significantly impacting the performance of information security
- **H2.** SOC is significantly impact in mediating the relationship between management support and information security performance

D. *Data Collection and Sampling Determination*

Data collection is done through surveys, which are conducted by distributing questionnaires to officials at selected banks randomly based on determining the sample design. The Likert scale used is 5 stages, namely Strongly Agree, Agree, Neutral, Disagree and Strongly Disagree. Likert scale is used, because it is one of the most widely used scales in business research [33].

While for SOC capabilities, measurements are based on the Capability Maturity Model [12], [26]. The Capability Maturity Model level used are:

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

The population of this study are banks in Indonesia. Based on data from the Financial Services Authority [34], there are currently 110 banks in Indonesia, so the total population of this study is 110. This study will use samples in the reference looking for data to be processed. The number of samples from this study uses a reference from Roscoe (1975), as cited in Sekaran and Bougie [33], where it is explained for multivariate based studies, the minimum sample size is 10 times the number of research variables. Because this study consisted of 3 variables, the minimum number of samples to be referenced was 30.

This is in line with the reference of the minimum number of samples from the SEM-PLS, ie the number of samples is determined by the number of the most arrows leading to a latent variable. With the highest number of arrows towards the latent variable is 2, with a significance level of 5% (in other words, the margin of error is 5%) and the value of R^2 is 0.25, then the minimum number of samples is 52 [35], [36].

The sample design used is a probability sample with disproportionate stratified random sampling. Stratified Random Sampling is a way of taking samples by paying attention to the strata (levels) in the population. In this design, the previous data is grouped into certain levels, such as the bank size. The next step is to randomly select each group [33], [37]. The banks are grouped based on size, which already determined by central bank regulation, called BUKU:

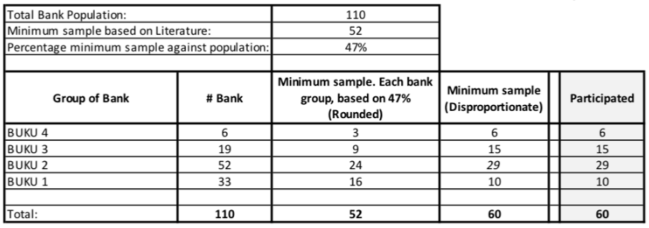
- **BUKU 1** Banks with core capital of less than Rp. 1 trillion (USD 71 Million), considered as very small bank.
- **BUKU 2** Banks with core capital of Rp. 1 trillion - Rp. 5 Trillion (USD 71 - USD 360 Million), considered as small bank.
- **BUKU 3** Banks with core capital of Rp. 5 trillion - Rp. 30 Trillion (USD 360 Million - USD 2.1 Billion), considered as big bank
- **BUKU 4** Banks with core capital above Rp. 30 trillion USD 2.1 Billion), considered as very big bank

Banks within every group above then selected randomly for survey. Unit analysis is bank, with respondents are bank employee with criteria as follow:

- Level: GM / Manajer / Section or Division Head / Supervisor
- Division: IT or IT Security
- Duration of work: Min. 3 years

The details of the number of participating banks are as shown in the table below:

Table 1. Disproportionate Random Sampling



Total Bank Population:	110
Minimum sample based on Literature:	52
Percentage minimum sample against population:	47%

Group of Bank	# Bank	Minimum sample. Each bank group, based on 47% (Rounded)	Minimum sample (Disproportionate)		Participated
BUKU 4	6	3	6		6
BUKU 3	19	9	15		15
BUKU 2	52	24	*29*		29
BUKU 1	33	16	10		10
Total:	**110**	**52**	**60**		**60**

All the data gathered from survey are analyzed using Structural Equation Modeling - Partial Least Square (SEM-PLS) method. SEM-PLS is a second-generation multivariate analysis method used to analyze and explain whether there is a relationship between latent variables from the study. In addition, SEM-PLS can also be used to confirm the previous theory, which underlies this research [35]. SEM-PLS has several advantages, such as the number of samples that do not need to be too large (at least 30), and do not need to be based on many assumptions and can be applied to all types of data scales [38]. this research is using SmartPLS v.3 software to analyzed data based on SEM-PLS method.

IV. RESULT AND DISCUSSION

A. *Model Evaluation*

The first thing we need to do related to our data analyzed using SEM-PLS is by evaluating our model, related to its validity and reliability. In SEM-PLS, **validity** is checked by examining convergent validity and discriminant validity, while **reliability** (Internal Consistency Reliability) is checked by the composite reliability and Cronbach's alpha. Convergent validity is determined by calculating value of outer loading of the model. The value of loading factors from indicators on latent variables must be greater than 0.5 as stated by Wong (2013) [35] and Chin (1998) as quoted in Ghozali and Latan [38].

As shown on the figure 2 below, the outer loading value of all indicator are above 0.5, meaning that all indicators are valid.

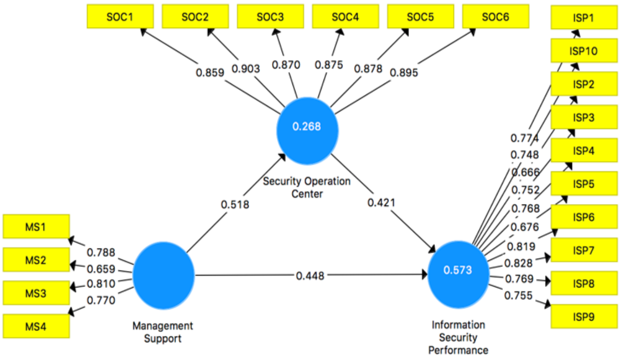


Figure 2. Loading Factor of the research model

Discriminant validity is determined by calculating the Average Variance Extracted (AVE). AVE value must be greater than 0.5, which means that 50% or more variance of the indicator can be explained [38], [39]. Meanwhile, reliability testing is done to prove the accuracy, consistency and determination of instruments in measuring constructs [38]. Based on several literatures, a construct is reliable if the Composite reliability and Cronbach's alpha are greater than 0.70 [35], [36], [38], [40]. The value of AVE, Composite reliability and Cronbach's alpha for each variable is on the table below:

Table 2. Validity & Reliability result

	AVE	Composite Reliability	Cronbach's Alpha
Information Security Performance (ISP)	0.573	0.930	0.917
Management Support (MS)	0.576	0.844	0.755
Security Operation Center (SOC)	0.774	0.954	0.942

Based on the table above we can conclude that all the variable are valid, since the AVE value of all variables are more than 0.5. The variables also reliable and can be used, since the value of Composite reliability and Cronbach's alpha are greater than 0.70.

B. *Hypotheses Testing*

In SEM-PLS, data is not considered normally distributed, which implies that the parametric test used in the regression analysis cannot be applied to test whether coefficients such as outer loadings, outer weights, and path coefficients are significant. In contrast, SEM-PLS relies on nonparametric bootstrap procedures to test coefficients for their significance [36]. Based on the output of bootstrapping we are able to know the significance of the indicators of each variable. Bootstrapping also needs to be done to obtain the t-value used to test whether the relationship between latent variables has a significant value or not. An indicator is declared significant, if the value of t-valuation is greater than 1.96 (z-score at confident interval (CI) 95% = 1.96). Based on the bootstrapping procedure as shown in the figure. 3 below we can consider all the indicators are significant, since the T-Value are more than 1.96.

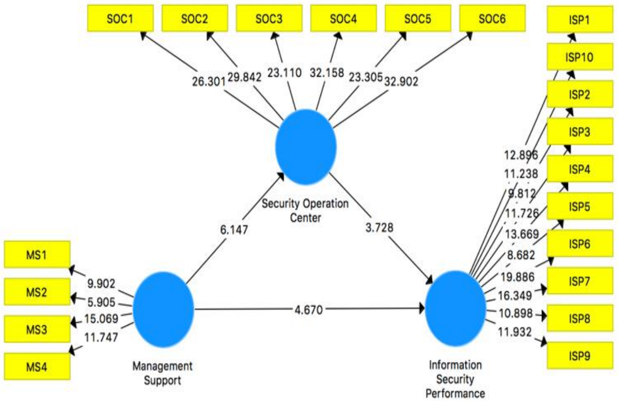


Figure 3. Bootstrap output of the model

After we find out that all the indicators are, valid, reliable, and significant, the next step is to test the hypotheses. The hypothesis in this study will be tested using the value of the coefficient path and t-values to see whether there is a significant influence or not of one exogenous and endogenous variable, on other endogenous variables. In addition, the results of testing the significance of the path also show the parameter coefficient value (original sample). The hypotheses testing for this research is stated on the table 3 below:

Table 3. Hypotheses Testing Result

Hipotheses		Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values	Remarks
H1	MS -> ISP	0.448	0.458	0.096	4.670	0.000	Accepted
H2	MS -> SOC	0.518	0.532	0.084	6.147	0.000	
	SOC -> ISP	0.421	0.416	0.113	3.728	0.000	
	MS -> SOC -> ISP	0.218	0.221	0.070	3.123	0.002	Accepted

Based on the results of the path coefficient at the table 3 above, the value of t-value of MS -> ISP is 4.670, this value is greater than 1.96 with a = 0.05. So that it can be concluded that hypothesis 1 (H1) is accepted, meaning that there is a significant effect of management support on information security performance. The influence of management support variables on information security performance has an original sample of 0.448 with a positive direction. This means that the better management support, the information security conditions will also increase.

For Hypotheses 2 (H2), we found that t-value of MS -> SOC -> ISP is 3.123, this value is greater than 1.96 with a = 0.05. So that it can be concluded that H2 is accepted, meaning there is a significant effect of SOC in mediating the relationship between management support and information security performance. In looking at the effect of SOC in mediating the relationship between management support and information security performance, a method from Hair et al. [41] will be used. What needs to be done is to examine the significance of the influence of exogenous variables in the relationship between MS-> SOC, SOC-> ISP and MS -> ISP. From the explanation in the sub-chapter of table 3 above, we find that MS-> SOC is significant (t-value: 6.147), SOC-> ISP is significant (t-value: 3.728) and MS -> ISP is also significant (t- value: 4,670). The table also shows that all three have positive values.

Retrieval Number: B3653078219/19©BEIESP
DOI: 10.35940/ijrte.B3653.078219
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Based on the explanation above, it can be concluded that the effect of SOC in mediating the relationship between management support and information security performance is significant and has partial or complementary mediation. Complementary mediation is a condition when direct or indirect influence is significant and goes in the same direction [41]. So that the better the capability of SOC, the relationship between management support and the condition of mediated information security will increase.

V. CONCLUSION & IMPLICATION

A. *Conclusion*

IT is a strategic component for the company, especially for the banking industry. IT is a business enabler, that is, businesses cannot run without IT. Therefore, IT implementation needs to be safeguarded so that it can be used in accordance with its functions. This study looks at how management support affects information security performance for companies. Management support empirically has significant impact on information security performance of the company. Therefore, we need to promote the awareness regarding the importance of information security to management level. This is not only because their support has significant impact, but also because information related asset owned by management level is very valuable and therefore become most targeted by attacker.

The other aspect that need to be considered to improve the performance of information security is by building Security Operation Center. This study confirmed empirically that SOC has significant impact on mediating the relationship between management support with information security performance, with complimentary mediation. Therefore, SOC is aligned with management support on improving information security performance of the company. Developing SOC will also need management support for it to be succeeded. In this study, one of the factors that differentiates and is novelty from previous research is the presence of SOC factors as one of the mediator variables.

For having its benefit, SOC do not have to be built and owned independently by the company. Independent development of SOC requires substantial costs, time and commitment. The alternative for companies that want to have SOC capabilities is to outsource these services to third parties. Companies can benefit from the existence of SOC, without having to bother with building SOC independently. This is in line with the recommendations of Muniz, McIntyre and AlFardan [12], for companies that want to benefit from SOC.

B. *Research Implication*

This research theoretically confirms and reinforces several previous studies. In the management support variable, this study confirms previous studies, and provides empirical data regarding the significance of its effect on information security conditions. For example, Torres et al. [7] states that management support is one of the key factors in information security. Furthermore, he states that management support is the most frequently mentioned aspect of information security, this is in line with the results of this study, that management support has a significant influence on the condition of information security.

Similar with above finding, the higher the level of management awareness and support for information security, as a whole will have an impact on the more efficient performance of companies related to IT security [10]. This study confirms and provides more valid empirical information, related to the influence of management support on the condition of corporate information security and the significance of that influence.

Regarding the SOC, this study provides the basis for further research, that the SOC has a positive and significant influence in mediating management support for information security conditions. With the nature of its mediation in the form of Complementary Mediation, the SOC has a greater influence than the relationship between management support and direct information security conditions. This can occur because both management support and SOC have a significant and positive influence on the condition of information security.

REFERENCES

1. B. King, Bank 3.0: Why Banking Is No Longer Somewhere You Go But Something You Do, 1st ed. Wiley, 2012.
2. R. Friedrich, A. Koster, S. Stroh, and C. Vollmer, “The 2012 Industry Digitization Index,” 2013.
3. Ponemon Institute, “2015 Cost of Cyber Crime Study: Global,” 2015.
4. ISACA, “State of Cybersecurity : Implications for 2015,” 2015.
5. PricewaterhouseCoopers, “The Global State of Information Security Survey 2016,” 2016.
6. N. Bradley, M. Alvarez, D. McMillen, and S. Craig, “2016 Cyber Security Intelligence Index,” 2016.
7. J. M. Torres, J. M. Sarriegi, J. Santos, and N. Serrano, “Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness,” pp. 530–545, 2009.
8. D. Willson, Cyber Security Awareness for CEOs and Management. 2016.
9. J. D. Jolley, “Article 2(4) and cyber warfare: How do old rules control the brave new world?,” Int. Law Res., vol. 2, no. 1, pp. 1–16, 2013.
10. N. Choi, D. Kim, and J. Goo, “Managerial Information Security Awareness’ Impact on an Organization’ s Information Security Performance,” in Americas Conference on Information Systems (AMCIS), 2006, p. Paper 406.
11. N. MacDonald and P. Firstbrook, “Designing an Adaptive Security Architecture for Protection From Advanced Attacks,” no. February, pp. 1–8, 2016.
12. J. Muniz, G. McIntyre, and N. AlFardan, Security Operations Center: Building, Operating, and Maintaining Your SOC. Indianapolis: Cisco Press, 2016.
13. C. Zimmerman, Ten Strategies of a World-Class Cybersecurity Operations Center. MITRE Corporation report release, 2014.
14. D. Nathans, Designing and Building Security Operations Center. 2015.
15. R. L. Krutz and R. D. Vines, The CISM Prep Guide: Mastering the Five Domains of Information Security Management, vol. 2003. Indianapolis, Indiana: Wiley Publishing, 2003.
16. I. Bernik and K. Prislan, “Measuring information security performance with 10 by 10 model for holistic state evaluation,” PLoS One, vol. 11, no. 9, pp. 1–34, 2016.
17. S.-M. Huang, C.-L. Lee, and A.-C. Kao, “Balancing performance measures for information security management: A balanced scorecard framework.,” Ind. Manag. Data Syst., vol. 106, no. 2, pp. 242–255, 2015.
18. E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown, and W. Robinson, “Performance Measurement Guide for Information Security,” NIST Spec. Publ., vol. 800–55, no. July, p. 80, 2008.
19. A. Kankanhalli, H.-H. Teo, B. C. Y. Tan, and K.-K. Wei, “An integrative study of information systems security effectiveness,” Int. J. Inf. Manage., vol. 23, no. 2, pp. 139–154, 2003.

20. T. Herath, H. Herath, and W. G. Bremser, “Balanced Scorecard Implementation of Security Strategies: A Framework for IT Security Performance Management,” Inf. Syst. Manag., vol. 27, no. 1, pp. 72–81, 2010.
21. D. Straub, “Effective IS Security: An Empirical Study,” Inf. Syst. Res., vol. 1, no. 3, pp. 255–276, 1990.
22. R. Werlinger, K. Hawkey, and K. Beznosov, “An integrated view of human, organizational, and technological challenges of IT security management,” Inf. Manag. Comput. Secur., vol. 17, no. 4, pp. 4–19, 2009.
23. Z. Tu and Y. Yuan, “Critical Success Factors Analysis on Effective Information Security Management: A Literature Review,” Twent. Am. Conf. Inf. Syst. Savannah, pp. 1–13, 2014.
24. S. M. Imroz, L. R. Pietron, D. A. Haworth, and K. W. Ward, “Application of Q-Methodology in Critical Success Factors of Information Security Risk Management,” vol. 7, no. 7, pp. 46–60, 2011.
25. Paul Burgin, “Whose customer are you? The Reality of digital banking,” 2019.
26. P. Jacobs, A. Arnab, and B. Irwin, “Classification of Security Operation Centers,” 2013 Inf. Secur. South Africa, pp. 1–7, Aug. 2013.
27. A. Michail, “SECURITY OPERATIONS CENTERS: A Business Perspective,” Utrecht University, 2015.
28. D. Kelley and R. Moritz, “Best Practices for Building a Security Operations Center,” Inf. Syst. Secur., vol. 14, no. 6, pp. 27–32, 2006.
29. H. Fulford and N. F. Doherty, “The application of information security policies in large UK-based organizations: an exploratory investigation,” Inf. Manag. Comput. Secur., vol. 11, no. 3, pp. 106–114, Jul. 2003.
30. N. Choi, D. Kim, J. Goo, and A. Whitmore, “Knowing is doing An empirical validation of the relationship between managerial information security awareness and action,” Inf. Manag. Comput. Secur., vol. 16, no. 5, pp. 484–501, 2008.
31. S. Kowtha, L. a. Nolan, and R. a. Daley, “Cyber security operations center characterization model and analysis,” 2012 IEEE Conf. Technol. Homel. Secur., pp. 470–475, Nov. 2012.
32. J. Y. Thong, C. S. Yap, and K. . Raman, “Top Management Support, External Expertise and Information Systems Implementation in Small Businesses,” Small Businesses Author Inf. Syst. Res., vol. 7, no. 2, pp. 248–267, 1996.
33. U. Sekaran and R. Bougie, Research Methods for Business: A Skill-Building Approach, 7th ed. WIley, 2016.
34. B. Indonesia, “Daftar Nama Kantor Pusat Bank di Indonesia,” 2017. [Online]. Available: http://www.bi.go.id/id/publikasi/laporan-keuangan/alamat-bank/umum/Default.aspx. [Accessed: 07-Jul-2017].
35. K. K. Wong, “Partial Least Squares Structural Equation Modeling (PLS-SEM) Techniques Using SmartPLS,” Mark. Bull., vol. 24, no. 1, pp. 1–32, 2013.
36. J. Joseph E Hair, G.Tomas M. Hult, Christian M. Ringle, and Marko Sarstedt, A primer on partial least squares structural equation modeling (PLS-SEM). California: SAGE Publications, 2014.
37. W. Zikmund, B. Babin, J. Carr, and M. Griffin, “Business Research Methods,” p. 668, 2009.
38. I. Ghozali and H. Latan, Partial Least Squares : Konsep, Teknik dan Aplikasi Menggunakan Program SmartPLS 3.0. Semarang: Badan Penerbit Undip, 2015.
39. J. F. Hair Jr, C. William, B. J. Babin, and R. E. Anderson, Multivariate Data Analysis. 2014.
40. R. B. Kline, Principles and practices of structural equation modelling. 2015.
41. J. F. Hair, G. T. M. Hult, C. M. Ringle, Sarstedt, and M., “A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM),” p. 363, 2017.

AUTHORS PROFILE

Toto A Atmojo. A Ph.D cadidate from Binus University Business School, Indonesia. He finished his bachelor degree in Informatics Engineering, Master of Computer in 2005, Master of Communication in 2007 and MBA in 2012. His main research focus are in Information Security and Management Information System. In professional life, he is now founder and CEO of www.defenxor.com, a cybersecurity company that helps organizations to improve their cyber security resilience.

Harjanto Prabowo. He is Professor of Information System Management and the President of Bina Nusantara University. He holds Doctoral degree from Padjajaran University and Master of Information System Management from Bina Nusantara University. His research focus is Strategic Knowledge Management and Innovation.

Idris Gautama So. He is a person with unique combination of professional, educator, business coach, facilitator, with engagement with related organizations. After working for companies in a prominent group of companies, he has dedicated most of his time this recent 15 years at Bina Nusantara University. He has been awarded him Associate Professor while now processing his Professorship. His papers have been published in proceedings and journals. Publications which has been indexed by Scopus can be found at https://www.scopus.com/authid/detail.uri?authorId=56007500000.

Sri Bramantoro Abdinagoro. He holds Doctoral degree from University of Indonesia, Magister Management from PPM School of Management and bachelor degree from University of Indonesia. Dr. Bram research are focusing on corporate and marketing management. He is currently a faculty member of Binus Business School in Jakarta, Indonesia.