Vol. 14(11), pp. 478-484, November, 2020
DOI: 10.5897/AJBM2019.8935
Article Number: 4A5936A65270
ISSN: 1993-8233

http://www.academicjournals.org/AJBM

ACADEMIC JOURNALS
expand your knowledge

African Journal of Business Management

Full Length Research Paper

The effects of organizational learning on the security of banking's information system in Indonesia

Said Herry Safrizal and Marjulin*

Politeknnik Negeri Lhokseumawe, Indonesia.

Received 14 November, 2019; Accepted 17 January, 2020

Organizational learning improves the security of information system. This study aimed to test and prove whether organizational learning had an effect on the security of information system. Data was gathered through survey, by administering questionnaires to public banks in Indonesia, and was tested using SEMPLS. This study employed explanatory research methodology. The findings showed that insecure information system was found to be the result of unoptimized organizational learning. In other words, organizational learning is a determining factor for a sufficient information system security.

Key words: Learning organization, security of information system.

INTRODUCTION

Eroğlu and Cakmak (2016) argue that security is a measure implemented to examine an entity's maturity in determining the potential risks and solutions for information system. Since information security cost in implementing new technology affects the external financial report and internal decisions, security is critical in creating quality information (Davis, 1996). Loch et al. (1992) note that the biggest risk to information system security comes from inside the enterprise. Furthermore, Spears and Barki (2010) found that at least half of information security breach cases was perpetrated by internal personnel. Users of enterprise's information system are often involved in risky behaviors that may harm the security and integrity of the organization, threaten to publish sensitive information, and weaken the publicly available technological security (Cox, 2012).

Security is indispensable. Security of information system is a measure to protect information from both internal and external threats (Albrechtsen, 2015). Because the majority of information systems are designed and made more flexible so that they are easily accessed by all groups, the impact on information system security becomes more lenient, so that it affects the security of the resulting information system, consequently system security will guarantee confidentiality, data integrity (integrity), and guaranteed availability of information when needed; availability also has an impact (Lachapelle and Bislimi, 2013). Wide-networked enterprises are prone to security risks, particularly on their application (Curtis and Cobham, 2008). Hence, system security needs to be more generally focused, involving more than mere antivirus and network security. It also needs to focus on the security of business transactions that involve valuable data. Information system design must be reliable and effective. It must implement the principle of timeliness and must be able

*Corresponding author. E-mail: julin_fira@yahoo.co.id.

to satisfy the required needs and quality. Information system must be affordable and secure (Bodnar and Hopwood, 2010).

Figure 1 displays the graph of bank security breaches by internal perpetrators based on the 2015 data from Indonesia's Banking Financial Service Authority.

Today's security problems involve highly-flexible security risks. Thus, security design must evaluate all aspects pertaining to system security and human factor in security policies (Solic et al., 2015). In other words, the problems of information security system are more than mere technological problems. The core of those problems is the human element. To identify risks in achieving and maintaining competitive advantages in a rapidly-changing business environment, organizational learning is highly crucial (Marquardt, 2002).

Ifinedo (2014) found that management can improve information system security by providing an environment in which individuals can learn organizational values. In line with that, Tan et al. (2010) argue that organizational learning is a process of learning from security incidents, in which compliance is the key to develop an effective security strategy.

Similarly, Schneider et al. (2012) note that organizational learning is a prerequisite for achieving better security in an organization. Furthermore, Cho (2007) argues that organizational learning involves a more intrinsic concept. To encourage system effectiveness review, an organization with good learning orientation will facilitate the implementation of new system.

The results of the research that have been done stated the need for effective learning to achieve a good system security situation, the problems that exist in Indonesia in particular and developing countries in general, organizational learning is still a problem that needs full attention.

In Indonesia in particular the strengthening of human resources through learning is still a problem that must be quickly addressed by the government (Baderi, 2014). Furthermore, Baderi (2014) said that the quantity of Indonesian human resources is indeed very young, but quality is still minimal, even the competitiveness of Indonesian human resources is still inferior to neighboring Malaysia. The same thing was also stated by Yanuar (2015) who stated that the level of education was still low with various problems; especially the quality of human resources needed attention and had to be addressed immediately.

LITERATURE REVIEW

Organizational learning is a process of knowledge acquisition and information implementation to adapt to changing situations. For an organization, learning involves knowledge acquisition, information dissemination, information interpretation, and organizational retention which successfully adapt itself to changing conditions. To put it simply, organizational learning involves behavioral changes based on organizational and personal experiences (Schermerhorn et al., 2010: 416).

Coghlan and Rashford (2006) argue that organizational learning is the process of learning aggregate on individual, teams, departments, and organizational levels. Organizational learning is defined as organizational ability to create, acquire, interpret, transfer, and disseminate knowledge, aiming to modify behaviors to reflect new knowledge and insight (Garvin, 2000: 11).

Organizational learning is based on the basic principles of learning, that is, acquiring and gathering information, interpreting it, and acting based on the interpretation of information (Garvin, 2000: 13). Organizational learning provides the principles and foundations for learning organization (Cleveland and Plantrik, 1995). Therefore, organizational learning is also described as a series of organizational behaviors that reflects a commitment to continuously learning and improvement.

Senge (1994: 3) notes that organizational learning has a strong orientation towards human resources. Furthermore, Baldwin et al. (1997) argue that members of all levels of an organization, not just the top management, continuously observe their environment to obtain key information; to change strategies and programs as needed to benefit from environmental changes, and to act with continuously improved methods, procedures, and evaluation techniques. Organizations that are willing to experiment and able to learn from their experiences will be more successful than those who are not (Wheelen and Hunger, 1986: 9).

Organizational learning is a vision of how an organization can become an ideal organization (Kofman and Senge, 1995) using five fundamental disciplines, each of which contributes to improving the organization's life and learning capacity. The five disciplines are personal mastery, awareness of mental models, building a shared vision, team learning and system thinking.

Boydell and Leary (1996) and Chaston et al. (1999) used and tested organizational learning model, which correlated with implementation, improvement, and integration, using 21 scale items from five dimensions: clear vision and mission, leadership commitment and empowerment, experimentation, knowledge transfer, and group problem solving. Baker and Sinkula (1999) measured and tested learning orientation using 18 items from three dimension, that is, commitment to learn, shared vision, and open-mindedness. Khandekar (2005) used 9 items to measure learning in its correlation with human resources activities. The nine items were: human resources strategy, training and education, performance evaluation, reward and incentive, conducive condition, work team, knowledge creation, management quality, and flexibility.

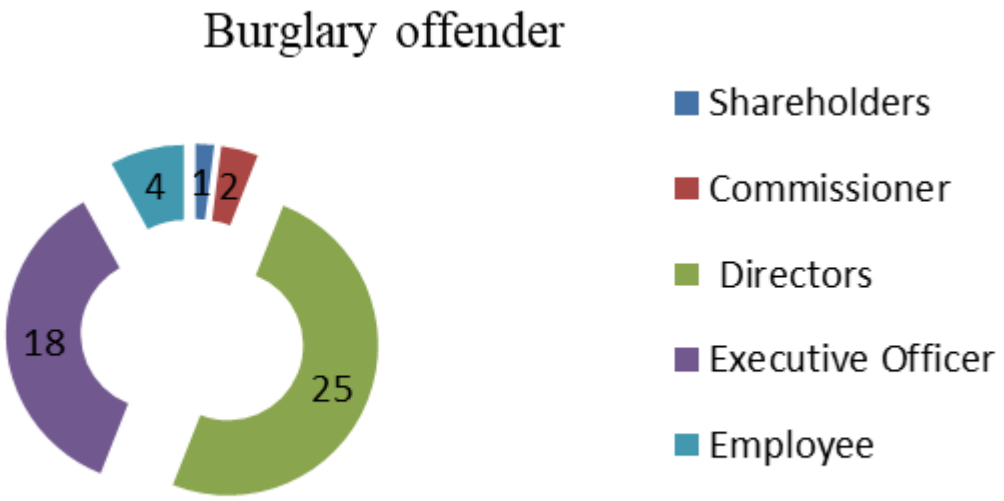

Figure 1. Burglaries in Indonesian Banking.
Source: OJK Financial Report (2015).

Table 1. Summary of second order validity tests on organizational learning variable.

Dimension	Factor weight	R^2	Error variance	T	CR	AVE
Thinking system	0.798	0.637	0.363	17.026		
Mental model	0.725	0.526	0.474	9.029		
Personal mastery	0.753	0.567	0.433	13.249	0.883	0.342
Team work	0.839	0.704	0.296	26.774		
Shared vision	0.647	0.418	0.582	9.152		

Information system security

Organizational dependence on information system keeps increasing. Information system security has become a critical issue for management in securing the organization, information system, and security risks caused by various interrelated internal and external factors (Feng et al., 2014). Anderson (2003) and Dhillon and Torkzadeh (2006) state that information system security is high-quality information which ensures that the risk from information source is appropriate to technical control, administration, and behaviors of the organization. Thus, information system security has become a core business process in any organization (Trcek, 2003).

Information system security can be viewed from risk-minimizing perspective. It means that information system security minimizes the risks that occur from inconsistent and incoherent behaviors in handling organizational information (Dhillon, 1995). This has caused an increase in concerns about organizational information assets protection (Dhillon and Backhouse, 2000). Todorov (2007: 1) sees information system security as an IT security; that is, information knowledge protects the assets from threats. Information asset is the smallest part of organizational or personal valuable information. The security of an information system is an attempt to protect the information system from various disturbances of people who want the information system to be damaged or broken, so that the information generated from the system is of quality (Table 1).

Garfinkel (1995) proposes that information system security covers four aspects: Privacy/Confidentiality, Integrity, Authentication, and Availability. Warkentin (2006: 10-11) argue that information system security is comprised availability, integrity, confidentiality, and authenticity elements. In line with this, Rathore (2004: 75) notes that information system security depends on three main criteria, that is, confidentiality, integrity, and availability (Table 2).

METHODOLOGY

This study employs descriptive and explanatory research methods. Sekaran and Bougie (2016: 123) argue that explanatory research is a study conducted to gather descriptions and systematic, factual, and accurate overview of facts, attributes, and correlation between variables. Organizational learning is the process of instilling in all members of organization the skills to identify problems and to find new ways to solve them in order to improve organizational effectiveness (Schermerhorn et al., 2010; Gephart and Marsick, 2016; Christensen et al., 2007). Based on various literatures and

Table 2. Summary of second order validity tests on information system security variable.

Dimension	Factor weight	R^2	Error variance	T	CR	AVE
Confidentiality	0.950	0.902	0.098	64.646		
Integrity	0.907	0.823	0.177	43.243	0.913	0.545
Availability	0.864	0.746	0.254	29.029		

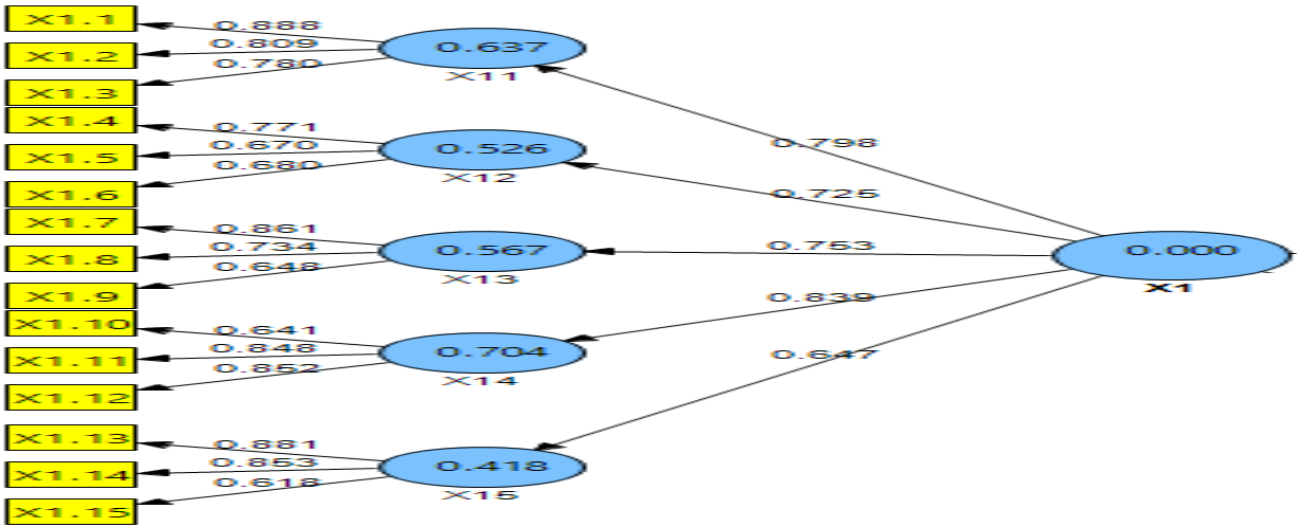

Figure 2. Path diagram of the measurement model for organizational learning variable.

theories, the concept of organizational learning is defined as appropriate and accurate data that supports information system security. Organizational learning in this study refers to learning process implemented by an organization to support its information system security.

Information system security is defined as all activities/processes of protecting information system and data contained in it from threats or misuse from unauthorized parties (Dhillon and Torkzadeh, 2006; Smith and Jamieson, 2006; Bodnar and Hopwood, 2006; Hall, 2011; Kim and Solomon, 2012; Laudon and Laudon, 2012).

Hypotheses

The hypothesis proposed in this study is that organizational learning has positive effects on information system security. The statistical hypotheses are:

$H_0 : \gamma_{11} \leq 0$; Organizational learning does not have positive effects on information system security.
$H_1 : \gamma_{11} > 0$; Organizational learning has positive effects on information system security.

The statistical test used in this study is:

$$t = \frac{\hat{\gamma}_{11}}{Se(\hat{\gamma}_{11})}$$

The test criterion is that H_0 is rejected if the p-value is smaller than the real value with a confidence level of 95% or an error rate of 5%.

FINDINGS AND DISCUSSION

Organizational learning is measured through 5 (three) dimensions, which are operationalized into 15 (fifteen) indicators. Data processing using second order confirmatory factor analysis yields a measurement model for the latent variable of organizational learning, as shown in Figure 2.

Information system security is measured through 3 (three) dimensions, which are operationalized into 9 (nine) indicators. Data processing using second order confirmatory factor analysis yields a measurement model for the latent variable of information system security, as shown in Figure 3.

The effect of organizational learning on information system security can be displayed as shown in Figure 4. Organizational learning is hypothesized to affect information system security. Table 3 displays the result of significance test of that hypothesis, using the following statistical hypotheses:

$H_0 : \gamma_{11} \leq 0$; Organizational learning does not have positive effects on information system security.
$H_1 : \gamma_{11} > 0$; Organizational learning has positive effects on information system security.

In Table 3, it can be seen that t_{calc} of organizational

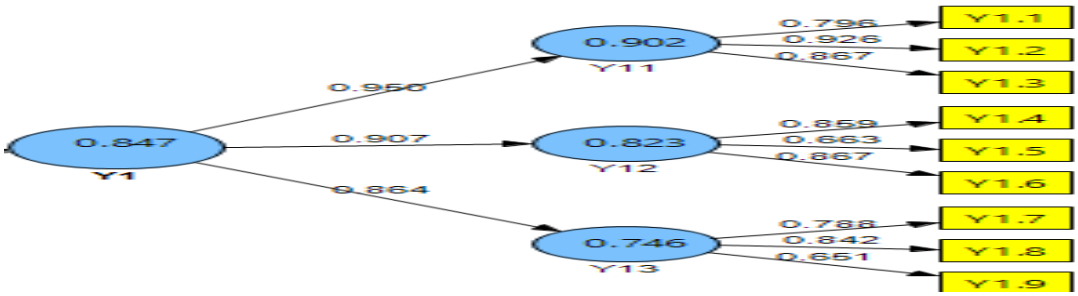

Figure 3. Path diagram of the measurement model for information system security variable.

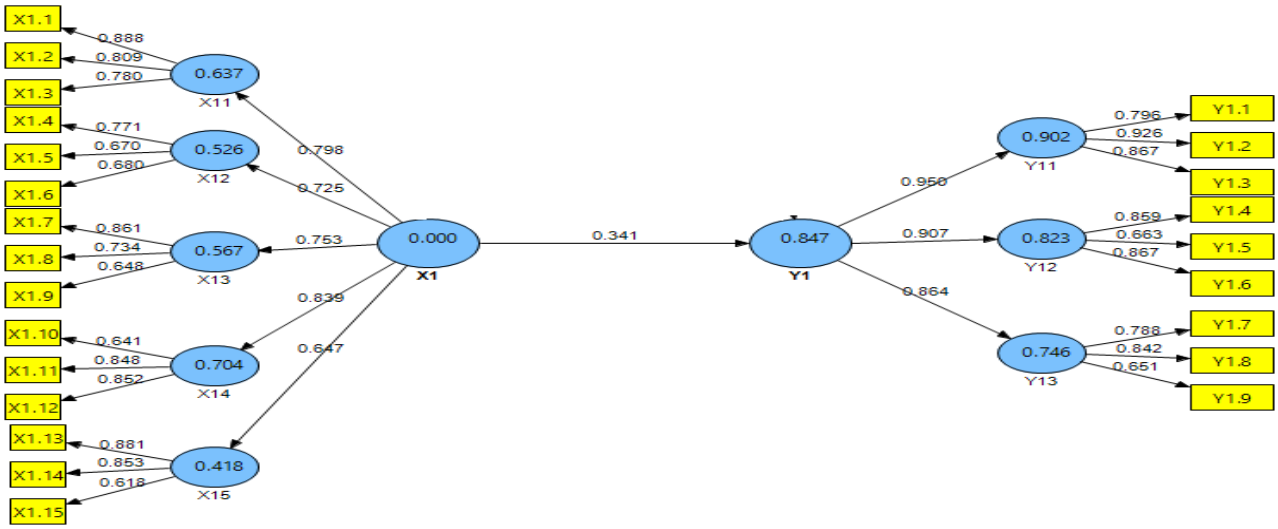

Figure 4. Path diagram of organizational learning's effect on information system security.

Table 3. Test Result of Organizational Learning's Effects on Information System Security.

Path Coef.	t_{calc}	t_{crit}	H_0
0.341	4.478	1.64	Rejected

learning variable (4.478) is greater than the t_{crit} (1.64). Since t_{calc} is greater than t_{crit}, on error variance of 5%, H_0 is rejected. Based on this result, it is concluded that organizational learning has significant and positive correlation to information system security in public banks. Considering the positive path coefficient, this finding provides an empirical evidence that the higher the level of organizational learning is, the greater the information system security will be. Organizational learning has a direct effect of 11.6% on information system security. To find the effect of size of organizational learning on information system security, the f^2 value is calculated. Data processing reveals that without organizational learning variable, the effect of users' competence and managerial commitment on information system security is 0.802. Hence, the f^2 value for organizational learning variable is:

$f^2 = R^2_{included} - R^2_{excluded} / 1 - R^2_{included} = 0.847 - 0.802 / 1 - 0.802 = 0.294$

f^2 is 0.294, indicating that organizational learning has moderate effects on information system security.

CONCLUSION AND RECOMMENDATIONS

Organizational learning positively correlates to information

system security because there are still some operational managers who do not get the opportunity for self-development because of a limited system of thinking, this limitation impacts that the limitations of the mental model of the manager will be disrupted, the impact on mastery of the manager is limited so that teamwork is not good, the concept is hampered from building a future vision of organization, the impact on members of the organization do not understand the assignment, especially to protect the information system from attacks/threats from external and internal parties who want to damage the information generated by the organization.

The results of this study support the research of Bartnes et al. (2016) who say that learning will enable organizations to improve response practices for incidents. Mattia (2011) said learning can help organizations to adapt and manage the process of securing organizational assets, and Kovacich (2016) states that system security is one of the fastest growing things now, the internet as a core infrastructure is the target of attacks, so organizations must have knowledge which is good for dealing with cyber-attacks through learning.

This study recommends improving organizational learning by implementing central banking policies concerning opportunities of self-improvement through further education and sustainable learning for members of banking institutions, and by formulating strategic plans for them to participate in seminar/workshops on information system security, to improve their understanding. In addition, banks are expected to implement the results of seminars and comparative study that are applicable to their organization.

Information system security improvement can be done by equipping the security system with firewalls, hiring information system security experts, developing secure applications that are readily applicable and adaptable to changing environment, and providing intensive instruction and trainings in information system security for members of the organization so that they will be able to handle any risks and threats to information system security.

CONFLICT OF INTERESTS

The authors have not declared any conflict of interests.

REFERENCES

Baderi F (2014). Low Quality of Indonesian Human Resources - New Government Challenges. http://www.neraca.co.id/article/45436/

Albrechtsen E (2015). Major accident prevention and management of information systems security in technology-based work processes. Journal of Loss Prevention in the Process Industries 36:84-91.

Anderson JM (2003). Why we need a new definition of information security. Computers and Security 22(4):308-313.

Baldwin TT, Danielson C, Wiggenhorn W (1997). The evolution of learning strategies in organizations: From employee development to business redefinition. Academy of Management Perspectives 11(4):47-58.

Baker WE, Sinkula JM (1999). Learning orientation, market orientation, and innovation: Integrating and extending models of organizational performance. Journal of Market-focused Management 4(4):295-308.

Bartnes M, Moe NB, Heegaard PE (2016). The future of information security incident management training: A case study of electrical power companies. Computers and Security 61:32-45.

Bodnar GH, Hopwood WS (2006). Accounting Information Systems, Tenth Edition. Upper Saddle River, New Jersey 07458: Pearson Education Inc.

Bodnar GH, Hopwood WS (2010). Accounting Information System (10th edition). United State America: Pearson Education Inc.

Boydell T, Leary M (1996). Identifying training needs (training essentials). London: CIPD.

Chaston I, Badger B, Sadler-Smith E (1999). Organisational learning: research issues and application in SME sector firms. International Journal of Entrepreneurial Behavior and Research 5(4):191-203.

Cho V (2007). A study of the impact of organizational learning on information system effectiveness. International Journal of Business and Information 2(1):127-158.

Christensen T, Lægreid P, Røvik KA (2007). Organization theory and the public sector: Instrument, culture and myth. Routledge.

Cleveland J, Plastrik P (1995). Learning, learning organizations, and TQM. Total Quality Management--Implications for Higher Education", College and University Personnel Association, (Forthcoming 1994).

Coghlan D, Rashford NS (2006). Organizational change and strategy: An interlevel dynamics approach. Routledge.

Cox J (2012). Information systems user security: A structured model of the knowing–doing gap. Computers in Human Behavior 28(5):1849-1858.

Curtis G, Cobham D (2008). Business information systems: Analysis, design and practice. Pearson Education.

Davis CE (1996). Perceived security threats to today's accounting information systems: a survey of CISAs. IS Audit and Control Journal 3:38-41.

Dhillon G, Backhouse J (2000) Information system security management in the new millennium. Journal Communications of the ACM 43(7):125-128.

Dhillon G (1995) Interpreting the Management of Information Systems Security: Doctoral dissertation. London School of Economics and Political Science.

Dhillon G, Torkzadeh G (2006). Value-focused assessment of information system security in organizations. Information Systems Journal 16(3):293-314.

Eroğlu Ş, Çakmak T (2016). Enterprise information systems within the context of information security: a risk assessment for a health organization in Turkey. Procedia Computer Science 100:979-986.

Feng N, Wang HJ, Li M (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. Information Sciences 256:57-73.

Garfinkel S (1995). PGP: Pretty Good Privacy: O'Reilly and Associates, Inc.

Garvin DA (2000). Learning in Action: A Guide to Putting the Learning Organization to Work. Boston, Harvard Business School Press.

Gephart MA, Marsick VJ (2016). Using Strategic Leverage Through Learning© to Address Organizational Challenges. In Strategic Organizational Learning. Springer, Berlin, Heidelberg. pp. 163-176.

Hall JA (2011). Accounting Information Systems Seventh Edition: South Western Cengage Learning, a part of Cengage Learning USA

Ifinedo P (2014). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. Information and Management Journal 51:1.

Yanuar RY (2015). Causes of Labor Productivity in Indonesia Low. Available at: http://ekbis.sindonews.com/read/1072141/34/

Khandekar S (2005). Organizational learning in Indian organizations: a strategic HRM perspective. Journal of Small Business and Enterprise Development 12(2):211-226.

Kim D, Solomon MG (2012). Fundamentals of information system security. Jones and Bartlett learning book and product are available through most bookstrores and online book sellers.

Kofman F, Senge PM (1995). Communities of Commitment: The Heart of Learning Organizations, Learning Organizations Chawla S, Dan J (eds.), Renesh, Oregon Productivity Press.

Kovacich GL (2016). The Information Systems Security officer's

Guide: Butterworth-Heinemann. USA.
Lachapelle E, Bislimi M (2013). ISO/IEC 27002. Information Technology Security Techniques Code Of Practice For Information Security Controls: International Standard ISO/IEC 27017.
Laudon KC, Laudon JP (2012). Management Information Systems Managing the Digital Firm Twelfth edition. by Pearson Education, Inc., Upper Saddle River, New Jersey, 07458.
Loch KD, Carr HH, Warkentin ME (1992). Threats to information systems: today's reality, yesterday's understanding. Mis Quarterly 1992:173-186.
Marquardt MJ (2002). Building the Learning Organization. New York: McGraw-Hill Companies, Inc.
Mattia A (2011). Utilizing a learning loop framework in IS security. International Journal of Business and Social Science 2:21.
Rathore B (2004). Information Systems Security Assessment Framework (ISSAF). Open Information Systems Security Group.
Schermerhorn JR, Hunt JG, Osborn RN, Uhl-Bien N (2010). Organizational Behavior (Elevent Edition). New York: John Wily and Sons. Available at: https://www.abebooks.com/book-search/author/uhl-bien-mary-schermerhorn-jr-john-r-osborn-richard-n/
Schneider K, Knauss E, Houmb S, Islam S, Jürjens J (2012). Enhancing security requirements engineering by organizational learning. Requirements Engineering 17(1):35-56.
Sekaran U, Bougie R (2016). Research methods for business: A skill building approach. John Wiley and Sons.
Senge PM (1994). The fifth discipline: the art and practice of the learning organization, 2nd edn. Bantam Doubleday.
Smith S, Jamieson R (2006). Determining key factors in e-government information system security. Information Systems Management 23(2):23-32.
Spears JL, Barki H (2010). User participation in information systems security risk management. MIS Quarterly 34(3):503-522.
Solic K, Ocevcic H, Golub M (2015). The information systems' security level assessment model based on an ontology and evidential reasoning approach. Computers and Security 55:100-112.
Tan TC, Ruighaver AB, Ahmad A (2010). Information security governance: When compliance becomes more important than security. In: IFIP International Information Security Conference pp. 55-67.
Todorov D (2007). Mechanics of user identification and authentication: Fundamentals of identity management. Auerbach Publications.
Trcek D (2003). An integral framework for information systems security management. Journal Computers and Security 22(4):337-360.
Warkentin M (2006). Enterprise Information Systems Assurance and System Security: Managerial and Technical Issues: Managerial and Technical Issues. IGI Global.
Wheelen TL, Hunger JD (1986). Strategic management and business policy. Addison-Wesley.