GADJAH MADA JOURNAL OF PSYCHOLOGY
VOLUME 6, NO. 2, 2020: 165- 177
DOI: 10.22146/gamajop.47415

ISSN 2407-7798 (Online)
https://jurnal.ugm.ac.id/gamajop

Cultivating Safety in the Information Technology Era

Endah Kumala Dewi[1], *Fathul Himam*[2], *Achmad Sobirin*[3]
[1,2]Faculty of Psychology, Universitas Diponegoro
[2]Faculty of Psychology, Universitas Gadjah Mada
[3]Faculty of Economy, Universitas Islam Indonesia

Submitted 8 July 2019 **Accepted** 30 June 2020 **Published** 27 October 2020

Abstract. In the information technology era, the banking industry must compete in an external environment characterized by high levels of uncertainty, complexity and change. Accidents in high-risk manufacturing organizations are generally related to safety studies. The researcher attempted to study "accidents" due to network vulnerabilities in IT-based organizations using the safety concept. This qualitative study is important because it provides analysis of IT support for organizational development. This study used multi-case study and grounded research approaches. The process of developing an information safety climate is considered an alternative solution other than technology. The study revealed that normal accident theory can be used to explain accidents in IT-based organizations. The process of developing an information security climate in banking organizations is categorized as the emergency type. The manifestation of information safety climate is attentiveness, accountability, ethical sensitivity, integrity and sustainability. Phases that need to be undergone in cultivating the safety climate are: adaptation, learning, awareness to risk, and resilience. Thus, it can be concluded that the climate of an IT-based organization is different from the climate of a non technology-based organization.

Keywords: banking organization; information; safety; security climate

People of the world are experiencing significant problems in maintaining the sustainability of organization. Franke (2011) stated that strategic environments e.g., politics, economic, defense, and socio-culture currently face threats namely volatility, uncertainty, complexity, and ambiguity (VUCA). Thus, the important things for organizations are to fulfill demands for information technology capacity and organization management in the face of uncertainty, ambiguity, and complexity of situations.

Information safety matters include threats and vulnerabilities that vary widely at this time. Various methods have been used to obtain information including storing and sharing information with other users. However, not all computer users always try to protect themselves when connected to another device. This raises a new challenge, namely information safety problem (Jaafar & Ajis, 2013).

Address for correspondence:
endahkd1963@gmail.com

A survey conducted by Kaleem and Ahmad (2008) found that bankers in Pakistan perceive electronics as tools to minimize inconvenience, reduce transaction cost, and save time in banking. However, Kaleem and Ahmad (2008) also found an evolving perception that electronic system opens up loopholes for information safety problems. This condition increases the chance of fraud and decreases security level (Nasution, 2012).

Castiglione (2002) said that banks have successfully protected their information assets in the cyber world using password, encryption, firewall, et cetera. Unfortunately, banks ignore security aspects of non-technical information e.g., documents accidentally found in the trash and left on a photocopy machine or employee's desk (Nasution, 2012).

Security and privacy risks in storing and sharing information are information safety problems transmitted over the internet. Privacy risk describes the extent of individual ability to control databases and the use of personal information. Security risk is a technical and administrative parameter to ensure personal information is not used by other people (Hiller, 2010).

Exploitation of information security is cyber threat in the form of various viruses or a collection of programs that can interfere with computer system. The threat can take form in malicious software (malware), irrelevant or inappropriate email sent to a large number of recipient (spam), software that enables user to obtain covert information about another's computer activity (spyware), the act of tricking someone through technology (social engineering), or stealing user data (phishing) (Arachchilage et al., 2014).

The pattern of information safety has shifted according to technology development. It started with protecting the confidentiality of hand-written information on telegrams to protection of informational content in phone conversations. In the latter development, information security matters are related to information sent through computers. Information safety needs to be placed as the main agenda to protect confidentiality of information distributed through the internet.

Information technology development affects every work process. We can see how various systems start with an 'e' e.g., e-commerce, e-voting, e-business, e-government, indicating that nearly all work mechanics are already digitalized. All communication processes in social interactions are also using digital devices e.g., personal digital assistant, smartphones, laptop, tablet pc, et cetera.

In the 21st century, hackers attack information safety by messing with computers for financial gain. This fact shows that nowadays nearly all industries' IT infrastructures are vulnerable to being penetrated by hackers. It also indicates the difficulty to identify attacker's presence in the computer system (Dlamini, et al., 2009).

Currently, nearly all working mechanisms are carried out online. For example, payment systems at various sales centers are conducted online which increase the popularity of electronic credit cards. This also encourages the development of

web-based applications. Even so, the statistics of hacking cases show that the new information technology development remains vulnerable and risky (Dlamini et al., 2009).

Studies found that individual as computer user is the weakest link in controlling information security (Arachchilage & Love, 2014). Many studies also indicated that solving information safety problems by only using technology is ineffective. Likewise, preventing threats to information security cannot solely depend on software development processes.

Normal Accident Theory was introduced by Charles Perrow after an accident at a nuclear power plant. He explained that an accident is preceded by local failure which spreads due to its interconnection with one another. Errors in complex and tightly connected system resulted in inevitable incident or failure in a specific unit. Failure that spreads and damages a specific unit will cause accidents or failures in the system or wider structure (Shrivastava et al., 2009). Human Error Model proposed by Reason (2000) aims to find the cause of error. It consists of two approaches. Person approach focuses on individual errors whereas Swiss cheese model focuses on the system approach to explain error caused by malfunction of various defense mechanisms in the system.

Studies on safety tend to focus on high-risk industries e.g., nuclear industry, traffic or health care industry (Glendon & Stanton, 2000; Graham & Harvey, 2001; Grote, 2007). In numerous literatures, implicit differences in the use of safety and security terms were found. Safety is related to accidents in the form of material risks or individual harms caused by the action of organization members. Security is related to threats from outside of the organization e.g., terrorism. In this study, safety and security have similar meaning within the information security context.

Most studies on information security disclosed issues from an organizational perspective. Large number of information security elements is unrelated to external threats, so experts lean towards the view that information safety problems are accidents within the company (Ilvonen, 2011). Based on that, organizations continue to identify potential risks related to information security and also implement policy in controlling information safety (Saint-Germain, 2005).

Efforts to identify potential risks are found in many studies. Security climate studies found that 78% cases were in the form of behaviors, such as intentionally opening attachments from unknown email addresses which later becomes medium of virus attack. Thus, information safety problems do not solely lie on IT systems but also in individual behavior (Chan et al., 2005).

Another example of information security risk is financial loss that occurred due to the breach of the information security system at Barings Bank. It illustrates weaknesses in audit and management techniques are not related to the IT system (Dhillon & Backhouse, 2001). Another risk factor is assumption made by various literatures about individual safety

behaviors that mediate the relationship between safety climate and safety system (Griffin & Neal, 2000). It can be concluded from those studies that the risk of information safety lies on the individual's behavior.

According to behaviorists, behavior is more important than other factors because it is observable so that attempt to control it can be exercised. A-B-C model is often used to explain behavioral safety (Kamp, 2011). Bandura described a phenomenon called observational learning as a learning process that emphasizes the anticipated consequences or things that one thinks will happen as a result of the behavior. In the 1970s, Bandura and other experts brought cognitive revolution in psychology. This paradigm focuses on the influence of thoughts, perceptions, attitudes, and values that drive emotions and behavior.

Based on explanations above, it can be gathered that safety problems in the globalization era are related to organization information safety. Information safety problems are found in IT-based organizations. Information security risks found in many studies are associated with individual behavior that cannot be separated from individual perceptions, attitudes, and values towards various internal situations of the organizations.

Individual appraisal of information safety problems in organization is obtained through perceptions towards organizational processes. These perceptions are developed through interactions with other individuals and the working mechanism of the organization. It results in a learning process to anticipate the consequences of their behavior and things that can happen in the organization.

Researchers of various studies have proposed developing a security climate. They show the importance in overcoming threats from inside of the organizations that are hidden and difficult to detect (Jaafar & Ajis, 2013). Many ideas that are oriented in security climate emerge e.g., workplace people centric (Dang-Pham, Pittayachawan, & Bruno, 2015) and High-Performance Work System (Zacharatos, Barling, & Iverson, 2005). The perception in the work environment is found to be able to detect the effect of safety climate in safety performance (Griffin & Neal, 2000).

Many studies have emphasized the role of technology in overcoming information security risks which are not necessarily effective in all organizational contexts. Study on the development of an organizational climate that focuses on information security is important because of the limited number of studies attempting to solve information safety problems to date. Thus, the question posed in this study is: what is the model of an organizational climate that promotes information security.

Method

In a research with study case approach, it is possible to use various data collection techniques according to research question formulation. Thus, data collection techniques and data analysis methods are very dependent on one another (Willig,

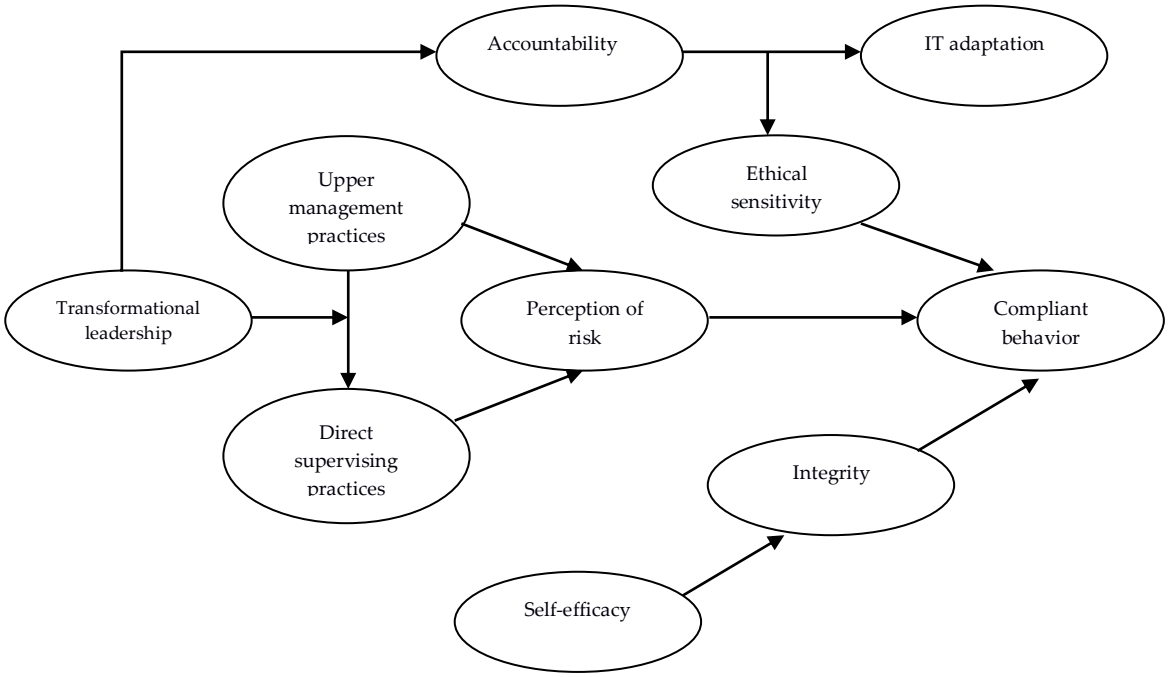

Figure 1. Dynamic process of information security climate development in state-owned Bank city Y and BSM city B

2008). In this study, two approaches were used: multi-case study and grounded research.

The main data sources in this study were in-depth interviews with respondents identified at the preliminary field study. Participants were six people working in national bank, insurance company, and rural bank (*Bank Perkreditan Rakyat*). The duration of this study was from early April 2018 to August 2018. This study presents qualitative data in narrative format. Description obtained is a construct of subjective experience and its meaning. Analysis process was done according to the analysis procedure introduced by Strauss and Corbin (1998), which consists of open coding, axial coding, and selective coding.

Results

Organizations participated in this study were state-owned bank city Y and BSM city B. The dynamic of information security climate development on both organizations is categorized as emergency type.

Descriptive explanation of Figure 1 is as follows: Emergency type is defined as the type of dynamic information safety climate development process where organization has reached a critical condition, namely fraud. Fraud is defined as the use of authority for personal gain e.g., to enrich oneself. Organizations need to take fraud prevention efforts immediately. Information security climate development process is initiated with actions from leaders with transformational leadership style to perceive fraud risk accurately and to ensure upper management and direct supervisors are having the same understanding. Those

perceptions used by leaders to determine the direction of organization.

Transformational leadership style is necessary to maintain organizational accountability through cultivating subordinates i.e., control process by upper management of supervisors. How the leaders work is firmly guided by ethical standards, namely standard operating procedures and company ethics. This results in organizational processes being tightly controlled.

Adaptation process of a new procedure, namely implementing an IT system, is encouraged by leaders. Leaders are able to sense when their subordinates cannot quickly adapt to the new procedure i.e., using a new IT system. One of the most important processes is leaders try to find lessons learned from previous problems. Leaders can train their subordinates to comply with prevailing standard procedure and ethics based on those experiences so as to maintain organization continuity. Leaders understand that it can open the door for violation of procedures and possibility of losing self-control at work. Nevertheless, leaders are able to foster organizational self-efficacy to continue to work with prudence and maintain integrity.

The dynamic process of information security climate development is described in Figure 2.

The initial step of establishing an organizational information safety climate is psychological readiness which contains awareness of the importance of information technology. This step is called the learning phase. This phase of change resulted in a mutual agreement that IT systems are an effective way of working because it facilitates work processes and protects customers; as stated by the following respondent:

> *"At the beginning of the establishment, banks did not use IT systems but used manual ways to record information instead. The decision to use IT systems along its development is needed to provide convenience in accessing customers' information…."* (W GN2 11-17)

The next step is the adaptation phase toward information security risks. The mechanism of adapting to work with IT systems generally occurs through an imitation process. The process occurs when employees follow coworkers' responses or comply with supervisors' instructions. Leaders also participate in controlling

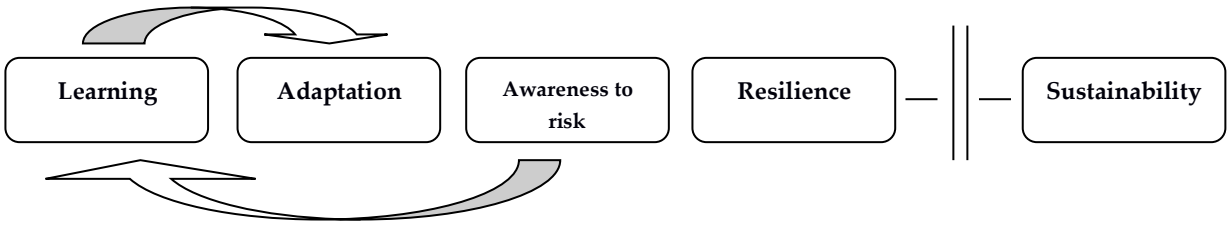

Figure 2. The dynamic phases of information security climate development in state-owned banks in Y City and BSM

employees' adaptation process to anticipate

changes in employees. The response example as follows:

> *"The concern is for example, we, in the company, there are rules, discipline as the basic ones, in the implementation not everyone doing the same, some of them comply and some of them disobey, even though we have conveyed it multiple times, socializing multiple times,…* (W NM 71-83)

Leaders shared information security risk through discussions to synchronize employees' perception in order to increase their competence; as stated by the following respondent:

> *"For daily routine, certainly there are clear rules, at most I communicate with them (employees), I monitor them, sometimes there are also sharing time, work time, it must be balance,…* (W NM 111-121)

Leaders embedded the right perception of information security risk through giving suggestions from upper management or supervisors by overtly imposing ethical values, company goals, and responsibilities.

The next step is awareness of information security risk phase through protection system and control from supervisors; as stated by respondent:

> *"In terms of transaction, the system will give warning, then authorization level, for example tellers only give withdrawal funds limit up to certain million rupiah, above that must be authorized by supervisor,…* (W SK 139-143)

Attempts to control behavior were carried out through dissemination of information system safety risk in order to foster alertness and organizational sense of belonging; as the following respondent's statement:

> *"We are now, with various kind of events—experiences the possibility of fraud from technology development, we prepare our field team, we keep on informing them then convey vicarious lesson learned so they will always be vigilant….* (W NM B 68-79)

The last step is the emerging organizational resilience phase, so that individuals can defend themself in the case of colleagues' abuse of power for their personal interests (fraud).

Developing individual resilience

Developing individual self-control ability; as stated by the following respondent:

> *"actually working in bank has many risks, risks mean risk from the company* (W GN1 108-117)

Individual developed ethical sensitivity; as stated by the following respondent:

> *"...we tried working in accordance with the procedures, working kindly and honestly… "*(W GN1 154-163)

Individual developed confidence to resist persuasion to commit fraud; as stated by the following respondent:

> *"in fact, if all the SOPs are carried out well, even though actually a bit loose, we*

> *(employees) already trust each other, we protect each other…"* (W GN1 181-190)

Developing resilience through organizational support

Organizations reframing information security risks perception through assertive leadership i.e. as the following respondents' statements:

> *"sharing moments develop obedience, belonging, and compliance to company values"* (W NM 244-261)
>
> *"leaders become role model who are close with employees, interacting, understanding , and monitoring employees' change"* (W NM 307-321)
>
> *"firmness to not accept any gifts from outsiders"* (W GN1 410-432)
>
> *"does not provide customers' personal information to other parties"* (W GN2 273-306)

Resilience was developed organizationally through operational control and ethical awareness:

> *"reminder from operational auditor regarding possible abuse"* (W GN2 365-373)
>
> *"developing ethical sensitivity using reward-punishment system"* (W GN2 273-306)

Discussion

This study aimed to discover the development process of information security climate in IT-based organizations. The results of data analysis found that organizational climate in IT-based organizations is different from the one in non-IT-based organization.

Nasution (2012) said that inappropriate use of information technology due to lack of socialization by the internal side of organization can damage the institution. Information technology plays an important role in effective and efficient banking operation. However, unethical use of information technology by internal part of organization can be counterproductive. Experts concluded that information technology and information security need to be regulated and in accordance with security standards i.e., confidentiality, integrity, and availability (Nasution 2012).

The organizations in this study were developing information security climate with emergency type. This suggested that the organizations have high awareness of information security risks. This is also influenced by critical situations because of abuse of power to enrich individuals of organizations from the past experiences. Even so, various socialization efforts were carried out frequently to instill information security values. Likewise, approaches to human resources were also made structurally and organizationally to anticipate information safety problems.

The results of data analysis showed that compliance is the finale target in the development process of information security climate. Vroom and Von Solms (2004) said that auditing employees' behavior in correlation with policy compliance is difficult, thus suggesting an unstructured and informal approach

according to organizational culture (Nasution, 2012). Bulgurcu and his colleagues (2010) examined the antecedent of employees' compliance with information safety policies in an organization and found that the effect of attitudes, normative beliefs, and self-efficacy on employees' intention to comply is significant (Nasution, 2012).

Aside from compliance, information safety policies also need to be developed. Baskerville and Siponen (2002) said the importance of safety policies formulation, particularly in organizations that have just started using information technology to implement and develop information security systems (Nasution, 2012). Leaders and management teams' involvement are important factors to create a secure atmosphere. Knapp et al. (in Nasution, 2012) found that upper management supports have a significant impact on information safety policies, law enforcement, and organizational security culture. Self-efficacy, lessons learned, ability to control behavior and work according to procedures were required during previous encounters with information safety problems.

This study showed that normal accident theory can be used to analyze accidents related to information security e.g., phishing or abuse of power. Accident process can be explained with normal accident theory and human error model. However, cognitive processes are also involved in human mechanisms that can cause incidents. Individual often adapt their behavior according to consequences experienced by others. Observational learning from Bandura can be applied as individual perception of information security risks.

Conclusion

Adhering to previous explanations, it can be concluded that the organizational factor that plays a role in controlling and managing organization to prevent accidents is the information security climate. Current study themes focused on safety in the workplace through interactions that take place in the workplace. It clarifies the importance of studying safety in the organizational environment setting. Therefore, information security climate is considered as an important construct organizational factor of behavioral safety.

Study by Ahlan, Lubis, and Lubis (2015) highlighted that training programs and performance of workmates have a significant role in the development of information security awareness. This study affirms the impact of the information security climate in Indonesia. Furthermore, studies also found that increasing self-efficacy as organizational psychological characteristics can enhance compliance toward information security rules (Chan, Woon, & Kankanhalli, 2005).

The psychological mechanism that occurs is initiated with the awareness of required information security (Jaafar & Ajis, 2013). After that, it follows by intention mechanism to obey information security policy (Stanton et al., 2005, Goo, Yim, & Kim, 2013). Individual who works in a team

with a positive information security climate will be motivated to engage in safety activities. After the intention mechanism to obey is developed, it is followed by imitation mechanism.

Based on explanations above, the development process of information security climate with emergency type can be described using Normal Accident Theory, human error model, and social learning theory. This study found the importance of information security climate that includes accountability, integrity, ethical sensitivity, perception towards risks, self-efficacy, transformational leadership role, and direct supervision. The impact of information security climate development is employees compliant to safety guidelines and policies (Chan, Kankanhalli, & Woon, 2005).

This study found cognitive processes involvement i.e., perception. Furthermore, involvement from leaders and supervisors affects the development of information security climate. This study also found that external supervision emphasizes on the importance of system's components to interact and influence one another. Information security describes protection and defense in IT systems to ensure that information is transmitted and stored securely, reliably, and efficiently (Schou & Trimmer, 2004).

Suggestion

From this study, it is found the need to formulate policy that can raise awareness of safety values, so that all organizational elements will uphold safeness based on awareness of maintaining the confidentiality of information.

Carelessness that occurs due to routine can increase risks to existing operational process i.e., incidents or near misses. If the risk of fraud is presented, it can cause a fatal accident. Organization will not only receive sanction from Financial Services Authority, but also will lose consumers' trust.

Acknowledgment. Researchers said many thanks to: 1) Ms. Tika, Mr. Andito, Mr. Gani, Ms. Nina Marlisa, and Mr. Saka as respondents; 2) Ni Putu Rizky Arnani as research assistant. 3) Ms. Nidya, Mr. Indra Bastian, Mr. Umam, Mr. Bobby Hamzar Rafinus, and Mr. Andy Ahmad Zailany as discussion partners.

Author's contribution. Endah Kumala Dewi wrote the manuscript.

Conflict of interest. Researchers do not have any kind of conflict interest with this study.

References

Ahlan, A. R., Lubis, M., & Lubis, A. R. (2015). Information security awareness at the knowledge-based institution: Its antecedents and measures. *Procedia Computer Science*, *72*, 361–373. doi: http://doi.org/10.1016/j.procs.2015.12.151

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer

users: A phishing threat avoidance perspective. *Computers in Human Behaviour*, *38*, 304–312. doi: https://doi.org/10.1016/j.chb.2014.05.046

Baskerville, R. & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management*, *15*(5/6), 337-346. doi: https://doi.org/10.1108/09576050210447019

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.

Castiglione, N. D. (2002). "My social security number is": Some common sense ways to fight identity theft. *ABA Banking Journal*, *94*(12), 57-59.

Chan, M., Woon, I., & Kakanhalli. (2005). Perceptions of information security at the workplace: Linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, *1*(3), 18-41.

Dang-Pham, D. Pittayachawan, S., & Bruno, V. (2015). Factors of people centric security climate: Conceptual model and exploratory study in Vietnam. Paper presented at The 26th Australasian Conference on Information Systems. University of South Australia, Adelaide.

Dhillon, G., & Backhouse, J., (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal*, *11*(2), 127-153. doi: https://doi.org/10.1046/j.1365-2575.2001.00099.x

Dlamini, M. T., Eloff, J. H. P., Elff., M. M., (2009). Information security: The moving target. *Computer & Security*, *28*, 189-198. doi: https://doi.org/10.1016/j.cose.2008.11.007

Franke, V. (2011). Strategic decision-making under uncertainty : Using case studies for teaching strategy in complex environments. *Journal of Military and Strategic Studies*, *13*(2), 1–21.

Glendon, A.I. & Stanton, N.A. (2000). Perspective on safety culture. *Safety Science*, *34*(1-3), 193--214. doi: https://doi.org/10.1016/S0925-7535(00)00013-8

Goo, J., Yim, M.-S., & Kim, D. J. (2013). A path way to successful management of individual intentions to security compliance: A role of organizational security climate. Paper presented at *Hawaii International Conference on System Sciences*.

Graham, J.R., & Harvey, C.R. (2001). The theory and practice of corporate finance: Evidence from the field. *Journal of Financial Economics*, *60*(2), 187-243. doi: https://doi.org/10.1016/S0304-405X(01)00044-7

Griffin, M.A., & Neal, A. (2000). Perceptions of safety at work: A framework for linking safety climate to safety performance, knowledge, and motivation. *Journal of Occupational*

Health Psychology, *5*(3). 347-358. doi: https://doi.org/10.1037//1076-8998.5.3.347

Grote, G. (2007). Understanding and assessing safety culture through the lens of organizational management of uncertainty. *Safety Science*, *45*(6), 637-652. doi: https://doi.org/10.1016/j.ssci.2007.04.002

Hiller, J. S. (2010). The regulatory framework for privacy and security. In J. Hunsinger, L. Klastrup, & M. Allen (Eds.) *International Handbook of Internet Research* (pp. 251–265). Dordrecht: Springer.

Ilvonen, I.(2011). *Information Security Culture or Information Safety Culture- What do words convey?* Paper presented at the 10th European Conference on Information Warfare and Security, The Institute of Cybernetics at the Tallinn University of Technology, Tallinn, Estonia. Academic Confereeces International Limited, 148-154.

Jaafar, I.N.,& Ajis, A. (2013). Organizational climate and individual factors effects on information security compliance behaviour. *International Journal of Busines and Social Science*, *4*(10), 118-130.

Kaleem, A. & Ahmad, S. (2008). Bankers' perception of electronic banking in Pakistan. *Journal of Internet Banking and Commerce 13*(1), 1-16.

Kamp, J. (2001). It's time to drag behavioral safety into the cognitive era. *Professional Safety*, *October*, 30-34.

Nasution, M, F, F, A. (2012). *Institutionalization of information security: Case of the Indonesian banking sector* (Unpublished doctoral dissertation). Virginia Commonwealth University, Richmond, Virginia.

Reason, J. (2000). Human error: Models and management. *BMJ*, *320*(7237), 768-770. doi: https://dx.doi.org/10.1136/bmj.320.7237.768

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC. 17799. The international information security standard provides a framework for ensuring business continuity, maintaining legal compliance, and achieving a competitive edge at the core. *Information Management Journal*, *39*(4). 60-62.

Schou, C. D., & Trimmer, K. J. (2004). Information assurance and security. *Journal of Organizational and End User Computing*, *16*(3), 1-13.

Shrivastava, S., Sonpar, K., & Pazzaglia, F. (2009). Normal Accident Theory versus High Reability Theory: A resolution and call for an open system view of accidents. *Human Relations*, *62*(9), 1357-1390. doi: https://doi.org/10.1177/0018726709339117

Stanton, J.M., Stam, K.R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computer & Security*, *24*(2), 124-133. doi:

https://doi.org/10.1016/j.cose.2004.07.001

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198. doi: https://doi.org/10.1016/j.cose.2004.01.012

Willig, C. (2008). *Introducing qualitative research in psychology* (2nd ed.). Berkshire: Open University Press.

Zacharatos, A., Barling, J., & Iverson, R. D. (2005). High-performance work systems and occupational safety. *Journal of Applied Psychology*, *90*(1), 77–93. doi: http://doi.org/10.1037/0021-9010.90.1.77