The European Proceedings of
Social & Behavioural Sciences
EpSBS

ISSN: 2357-1330

https://doi.org/10.15405/epsbs.2019.08.51

ICBSI 2018
International Conference on Business Sustainability and Innovation

THE EFFECTS OF CYBER SUPPLY CHAIN RISK MANAGEMENT IN FINANCIAL INDUSTRY

David Yeoh Beng Tatt (a)*, Yuvaraj Ganesan (b),Yudi Fernando (c)
*Corresponding author

(a) Graduate School of Business, Universiti Sains Malaysia, Penang, Malaysia, davidyeoh71@gmail.com
(b) Graduate School of Business, Universiti Sains Malaysia, Penang, Malaysia, yuvaraj@usm.my
(c) Universiti Malaysia Pahang, Pekan, Pahang, Malaysia, yudhitjoa@gmail.com

Abstract

Cyber security had been a major concern for all market industry especially on the financial industry services sector. Cases of cyber fraud had been reported all over the world including Malaysia and had caused billions of financial losses ruined as well as reputation which are at risk until now. Therefore, this study analyzed the cyber supply chain risk management (CSCRM) which comes into effect that will have an impact on the financial performance with mediating effects of cyber-resilience and service performance on the financial industry. Data collection is based on an online survey questionnaires (structured questionnaires) designed and published which is distributed from the list of respective individual managers involved in operations and Information Technology (I.T.) in the financial institutions industry in Malaysia. The research methodology used in this study is to test the relationship whether significant or insignificant between cyber supply chain risk management, financial performance, cyber-resilience, service performance, financial performance, as well as mediating variables effects of cyber-resilience and service performance while addressing the research questions with the following hypothesis proposed. In a nutshell, cyber supply chain risk management is designed to handle cyber risks which were caused by attacks from outsiders or the failure to manage risks internally in terms of governance, systems integration and operations and its impacts towards financial performance.

Keywords: Cyber supply chain, risk management, financial performance, cyber-resilience, service performance.

https://doi.org/10.15405/epsbs.2019.08.51
Corresponding Author: David Yeoh Beng Tatt
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

The widespread used of internet banking had resulted in the new dependence upon computer systems and data captured within. As a result, computers contains millions of database records relating to commerce, healthcare, banking, defence and even our personal information. With all these information recorded and captured in the computer systems, it is a risk of either being misused for fraudulent purposes or information modified for malicious reasons. At the same time, the vulnerability of these systems to attack from malicious individuals or groups is growing tremendously in all over the world.

1.1. Background of the study

Cyber security is generally recognized as a critical priority within the nation of a country, and in the business security communities as well. Governments all over the world have begun to show sign of concerns from the threat to their global supply chain for Information and Communications Technology (ICT) products aspects. These concerns are based on the risk that an opposition might tamper with products during their development, manufacture, production or even during delivery stage. In answering to these concerns, some governments have begun to establish policies and requirements which are intended to reduce these supply chain risks.

This view on the cyber threat has been reflected at the highest levels of the U.S. government, stating that "*cyber threat is one of the most serious economic and national security challenges we face as a nation.*" (Obama, 2009) According to a report conducted by the Malaysian cybersecurity agency, it was quoted that "more than 2,100 servers in Malaysia have been compromised and hacked" (Mu, 2017). Most of these servers belong to government agencies, banks, universities and businesses from the market industry.

Definition

Author	Definition/characteristics of "cybercrime"	Internet fraud	Computer hacking	Cyber piracy	Spreading of malicious code	Others
Thomas and Loader [27]	Illegal *computer-mediated activities* which can be conducted through global electronic networks.	✔	✔	✔	✔	✔
Richards [20]	The illegitimate use of *computer* to conduct criminal activities.	✔	✔	✔		✔
Parker [15]	Encompasses any abuse and misuse of information that entails using knowledge of *information systems*.	✔	✔	✔		✔
Philippsohn [16]	Criminal activities conducted through the *Internet*.	✔	✔	✔	✔	
Power [19]	The intentional access of a *computer* without authorization or by exceeding authorization and thereby obtain information to which the person is not entitled.	✔	✔	✔	✔	✔

Figure 01. An overview of cyber crimes Source: Chung et al. (2006)

Figure 01 shows an overview of cyber crimes with the definition and characteristics of "cybercrime" (Chung, Chen, Chang, & Chou, 2006). Due to that, cyber resilience is becoming increasingly recognized as a critical component of comprehensive cyber security practices. Cyber resilience can be described as a cyber-system's ability to function properly and securely despite disruptions to that system. Disruptions can be cyber or physical; they can also be intentional, accidental, or random. Therefore, cyber supply chain risk management (CSCRM) is an integrative discipline combining elements of cyber security, supply chain

https://doi.org/10.15405/epsbs.2019.08.51
Corresponding Author: David Yeoh Beng Tatt
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

management, and enterprise risk management into a new and powerful concept to exert strategic control over the end-to-end processes of the focal organization and its extended enterprise partners (Boyson 2014).

Cyber supply chain can be defined as an end to end integration of supply chain over secured and intricate digital network (Gani & Fernando, 2018). The whole set of main performer using cyber infrastructure such as network, information system, system integrators and software or hardware suppliers.

Therefore, service performance measurement is regarded as important due to the increasing significance of service activities, but it is also regarded as a more complicated one compared to the manufacturing context (Pawar, Beltagui, & Riedel, 2009). The risks management and concerns over the threat had actually affected the public as well as the image and reputation of the financial institutions industry as a whole.

Figure 02 presents some of the local and foreign banks in the financial institutions industry that offered internet banking or e-banking services in Malaysia which also comprises the top 9 local banks in Malaysia as well (Hamid, Amin, Lada, & Ahmad, 2007).

LOCAL BANKS
1. Alliance Bank Malaysia Berhad
2. Am Bank (M) Berhad
3. Bumiputra Commerce Bank Berhad
4. Bank Islam Malaysia Berhad
5. Hong Leong Bank
6. Malayan Banking Berhad
7. Public Bank Berhad
8. RHB Bank Berhad
9. Southern Bank Berhad
FOREIGN BANKS
1. Citibank Berhad
2. HSBC Bank Malaysia Berhad
3. OCBC Bank (Malaysia) Berhad
4. United Overseas Bank (M) Berhad

Figure 02. Banks offering internet banking services in Malaysia (Source : Hamid et. al., (2007))

1.2. Overview of financial industries in Malaysia

Malaysia's financial sector is well diversified. It comprises banking intermediaries, insurance companies and capital market intermediaries with overall assets of close to 400% of GDP as of end-2011 (International Monetary Fund, 2013). There are 53 banking intermediaries, accounting for around 50.6% of the financial system's total assets. Malaysia has 23 commercial banks, 16 Islamic banks, and 14 investment banks.

The Malaysian financial system has played an important catalytic role in facilitating the economic transformation and growth of the Malaysian economy through the various phases of economic

https://doi.org/10.15405/epsbs.2019.08.51
Corresponding Author: David Yeoh Beng Tatt
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

development. The use of internet technologies in the financial system and the application of internet technologies to businesses for improvements in their performances are not something new.

As stated by (Saffu, Walker, & Hinson, 2008), there is an increase in applications of e-commerce in businesses in the past ten years. The benefits of e-commerce include reduction in cost, increasing business opportunities, reducing lead time and providing a more personalized service to the consumers (Turban, King, Lee, Warkentin, & Chung, 2006). One e-commerce tool that is being adopted by the banking industry is online banking or better known as e-banking. Information technology tools such as online banking or e-banking have provided an improvement in services among the banking industry (Dawes & Rowley, 1998). At present, there are more than thousands of e-banking websites all over the world (Guraau, 2002). Although online banking has been implemented in many developed countries such as the United States and those in Europe (Pikkarainen, Pikkarainen, Karjaluoto, & Pahnila, 2004), there is a sign of growing trend in the adoption of online banking or e-banking by banks in emerging countries as well like Malaysia (Guraau, 2002).

Thus, internet banking or online banking had become one of the popular wider spectrums that support the functioning of the financial industry economy and its transformation as a whole. Therefore, the security issue on the internet banking system should not be taken lightly as it will eventually affect the financial performance of the organization if cyber fraud were to take place.

According to (Ganesin, Supayah, & Ibrahim, 2016) the reported incidents of cyber crime recorded by Cyber999 in Malaysia increased from 3,564 cases in 2009 to 8,090 cases in 2010. The reported cyber crimes increased 127% within one year period. As of November 2011, the total number of reported cyber crimes was 14,157. This is hard evidence that shows cyber crimes are increasing at an alarming rate. According to Lt Col (Rtd) Prof Datuk Husin Jazri, the CyberSecurity Malaysia chief executive officer, until August 2011, there were 10,000 cases reported every month in Malaysia (Muniandy & Muniandy, 2012).

Furthermore, Malaysia has experienced over 10,000 cyber incidents in 2015 and expects increased commercial fraud, ransomware and online scams in 2016 and 2017. According to Dr. Amiruddin Abdul Wahab, CEO of CyberSecurity Malaysia, the Internet of Things (IoT) can be link to security challenges for business enterprises and customers.

This lead to the cyber supply chain which is an end-to-end process that involves people, process and technology which is similar like the product supply chain. (Boyson, Corsi, & Rossman, 2009) denotes that cyber supply chain as “the entire set of key actors and their organizational and process-level interactions that plan, build, manage, maintain, and defend the IT system infrastructure”. This is the same factors that drives the growth of cyber supply chain risk management to handle cyber risks which are related to governance, systems integration and operations respectively and its impacts on the financial performance.

2. Problem Statement

The reputation of financial firms for being secure is of critical importance, both for the firm and its customers. Financial institutions have a very large economic incentive to assure the security of their information. As a result, financial firms are very proactive about security and business continuity.

https://doi.org/10.15405/epsbs.2019.08.51
Corresponding Author: David Yeoh Beng Tatt
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

In addition to that, the cyber supply chain remains as the weakest link as it is mainly targeted by ransomware (CyberSecurity ASEAN, 2018). Therefore, a study is required to assess to what extent the bank is equipped for online banking transactions.

- The core issues or problems in this research paper are how to best deal with risk and uncertainty.
- This paper focuses on the severity of the cybercrime such as phishing on the Malaysian banking industry as it is ever constant looming threat upon the banking service industry (Gan, Ling, Yih & Eze, 2008).
- There are concerns relating to unintended access to supply chain information by unauthorized third parties (Rieback, Crispo, & Tanenbaum, 2006); Cai, Jun & Yang, 2010); (Kim, 2013) and disrupting the flow of information (Chopra & Sodhi, 2004); (Dynes, 2008); (Jones & Horowitz, 2012). This is because there is an increasing number of Malaysians who have transactions online (Ali, Samsuri, Sadry, Brohi, & Shah, 2016).
- This study will address the growing concern about information systems (IS) misuse, especially with Web-based systems (D'Arcy & Hovav, 2007). The explosive growth of the Internet has brought about an escalation of security concerns about IS misuse, specifically cyber misuse (Siponen, 2005).

3. Research Questions

1. Is there a positive relationship between cyber supply chain risk management and financial performance?
2. Does cyber supply chain risk management have significant effect on cyber-resilience?
3. Is there a positive relationship between cyber supply chain risk management and service performance?
4. Is there a positive relationship between cyber-resilience and financial performance?
5. Is there a positive relationship between service performance and financial performance?
6. Does the cyber-resilience mediate the relationship between cyber supply chain risk management and financial performance?
7. Does the service performance mediate the relationship between cyber supply chain risk management and financial performance?

3.1. Research Objectives

The objectives of this study focused on financial performance through the direct effect of cyber risk in the supply chain that explains the relationship between variables (independent and dependent variables together with mediator variables such as cyber-resilience and service performance).

Among the objectives that will be highlighted in this study are as follows:-

1. To examine the relationship between cyber supply chain risk management and financial performance
2. To examine the relationship between cyber supply chain risk management and cyber-resilience

https://doi.org/10.15405/epsbs.2019.08.51
Corresponding Author: David Yeoh Beng Tatt
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

3. To examine the relationship between cyber supply chain risk management and service performance
4. To examine the relationship between cyber-resilience and financial performance
5. To examine the relationship between service performance and financial performance
6. To examine whether the cyber-resilience mediate the relationship between cyber supply chain risk management and financial performance
7. To examine whether the service performance mediate the relationship between cyber supply chain risk management and financial performance

4. Purpose of the Study

Cyber supply chain risk management is an emerging topic in the risk management research. Organizations interact with their customer, supplier and business via IT network and information system to improve supply chain performance. Previous scholars have proven that collaboration and integration among business partner can improve firm supply chain performance. Hence, managing cyber risks or information security risks is very crucial for firm to achieve highest performance. This study is among the pioneer empirical study on the effect of cyber supply chain risk management on financial performance with mediating effects of cyber-resilience and service performance. This could make several significant contributions to the industry and practitioner. There are two contributions to this study (i.e. theoretical significance and practical significance).

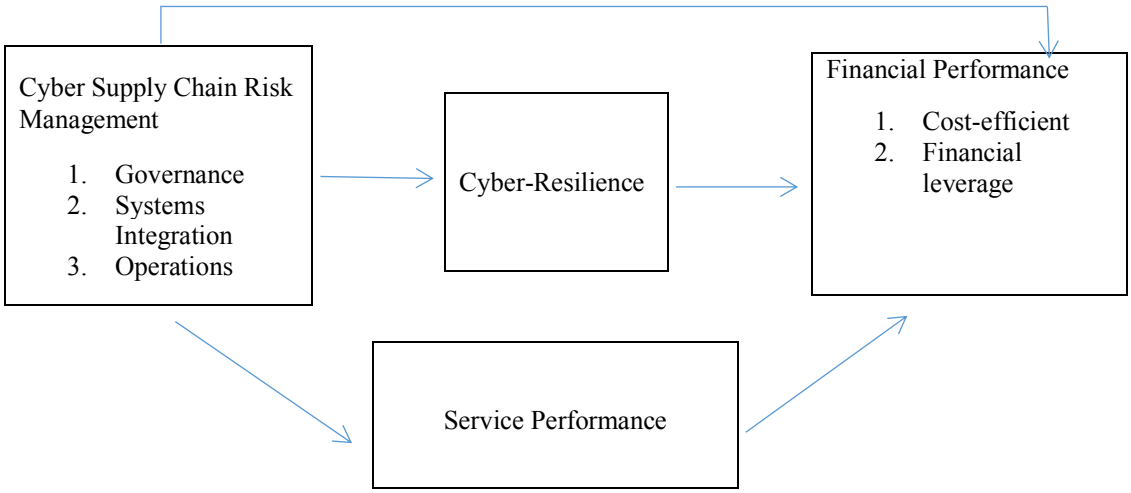

Figure 03. Theoretical Framework

4.1. Independent variables - Cyber supply chain risk management

The cyber supply chain risk management involves measures such as governance, systems integration and operations (Boyson, 2014). This paper was an extension of a study conducted by Boyson et al. (2009) and Simpson (2010), who defines the IT system supply chain as a globally distributed dynamic collection of people, process, and technology.

https://doi.org/10.15405/epsbs.2019.08.51
Corresponding Author: David Yeoh Beng Tatt
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

4.2. Dependent variables - Financial performance

The Dependent Variable is the financial performance of the bank which can be measured through various key indicators such as return on assets (ROA) and loan losses to total loans. Return on assets measures the ability of bank managers to acquire deposits at a reasonable cost, invest these funds in profitable loans and investments, and profitably perform the daily operations of the bank. The variables consists of cost-efficient and financial leverage.

4.3. Mediator - Cyber resilience

Cyber-resilience is the ability of an organization to prevent, detect, respond and recover from the impacts of an attack with minimal damage to their reputation and competitive advantage (Wilding, 2016). Hence, an organization should have a built-in cyber-resilience to prevent from any cyber-attack from internal or external parties. In the previous research conducted by Avery & Ranganathan (2016), it was stated that information security breaches can impact the market value of an organization because of the reputation of the organization had been jeopardized while market assumes that revenues will decrease and expenses will increase. The result will impact the financial performance of the organization such as Return on Sales (ROS), Return on Assets (ROA) and Return on Investment (ROI), (Ravichandran & Lertwongsatien, 2005; Santhanam & Hartono, 2003).

4.4. Mediator - Service performance

A proper definition for service performance from the customers' viewpoint is "the perceived quality of a given service against the actual service outcome (Grönroos, 1984). This service performance relates to behaviors that will increase the desired outcomes by serving and helping the customer (Bowen & Waldman, 1999; Liao & Chuang, 2004). Some of the examples of service performance behavior comprises on asking questions, giving suggestions and listening to customers' needs (Borucki & Burke, 1999). As a matter of fact, this kind of service performance is known as an abstract idea of extra-role performance (Williams & Anderson, 1991). According to Ladhari et al., (2015), reported that both perceived service quality (reliability, responsiveness, assurance, and empathy) and service environment (atmosphere and layout) will increase positive emotional satisfaction.

5. Research Methods

The review of the type of research design, data collection method, survey instrument, measurement of variables, data analysis is included in the dissertation. This study is to examine how all these research methods tested will have any significant or insignificant relationship with each other one way or another.

5.1. Descriptive and qualitative research design

A descriptive and qualitative research design was chosen to evaluate the relationship between cyber supply chain risk management and financial performance along with the possible mediator factors of service performance and cyber resilience. More specifically it would address the following research question: Is

https://doi.org/10.15405/epsbs.2019.08.51
Corresponding Author: David Yeoh Beng Tatt
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

there a causal relationship between cyber supply chain risk management with the financial performance of the bank?

5.2. Structured questionnaires

The study will be carried out using survey with structured questionnaires which will be published on a webpage as well as hard copy which will be distributed to the respective operations and I.T. managers in the financial institutions. Gathering of primary data first hand based on communication with a sample of individual parties and thereafter compiled specifically for this study (Zikmund, 2003).

- The methodology employed in obtaining information about customer satisfaction level of the bank chosen on the importance of cyber supply chain risk management via a survey conducted at a sample of the specific IT managers of the banking industry. The survey questionnaire is also design and distributed to obtain direct answers from the experts of the IT managers who deal with cyber security threats in retail banks of Penang.

6. Findings

The findings will be based on the sample data gathered and collected for testing. A hypothesis test will also be conducted based on the evaluates of two mutually exclusive statements about a population to determine which statement is best supported by the sample data.

7. Conclusion

CSCRM is a topic which is increasingly receiving attention from the public due to the recent issues of cyber fraud in the marketplace and challenges faced by the financial institution organization.

This paper contributes to the objective focused on through the direct effect of cyber risk in the supply chain that explains the relationship between variables (independent and dependent variables together with mediators).

Cyber supply chain risk management is designed to handle cyber risks which were caused by attacks from outsiders or the failure to manage risks internally in terms of governance, systems integration and operations and its impacts towards financial performance. It also involves mediator variables such as cyber-resilience and service performance as well.

This study also emphasizes on the financial impact besides revenue, operating costs, and working capital under the financial performance aspects, it is also believed that an effective SCM can also be expected to impose positive contributions towards *dependent variables such as cost-efficient and financial leverage* based on a research methodology conducted. When this study is completed, we will be able to measure the hypothesized relationships outlined in this paper and subsequently be able to provide a detailed key research and practical implications which will include suggestions for future research as well.

References

Ali, N. I., Samsuri, S., Sadry, M., Brohi, I. A., & Shah, A. (2016). *Online shopping satisfaction in Malaysia: A framework for security, trust and cybercrime.* Paper presented at the Information and

Communication Technology for The Muslim World (ICT4M), 2016, 6th International Conference on.

Avery, A., & Ranganathan, C. (2016). Financial Performance Impacts of Information Security Breaches.

Borucki, C. C., & Burke, M. J. (1999). An examination of service-related antecedents to retail store performance. Journal of organizational Behavior, 943-962.

Bowen, D. E., & Waldman, D. A. (1999). Customer-driven employee performance. Pulakos (Eds.), The changing nature of performance, 154, 191.

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation, 34*(7), 342-353. doi: 10.1016/j.technovation.2014.02.001

Boyson, S., Corsi, T., & Rossman, H. (2009). Building a cyber supply chain assurance reference model. *Science Applications International Corporation (SAIC)*.

Cai, S., Jun, M., & Yang, Z. (2010). Implementing supply chain information integration in China: The role of institutional forces and trust. *Journal of Operations Management, 28*(3), 257-268.

Chopra, S., & Sodhi, M. (2004). Supply-chain breakdown. *MIT Sloan management review, 46*(1), 53-61.

Chung, W., Chen, H., Chang, W., & Chou, S. (2006). Fighting cybercrime: a review and the Taiwan experience. *Decision Support Systems, 41*(3), 669-682.

D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM, 50*(10), 113-117.

Dawes, J., & Rowley, J. (1998). Enhancing the customer experience: contributions from information technology. *Management decision, 36*(5), 350-357.

Dynes, S. (2008). *Emergent risks in critical infrastructures.* Paper presented at the International Conference on Critical Infrastructure Protection.

Gan, G. G. G., Ling, T. N., Yih, G. C., & Eze, U. C. (2008). Phishing: A growing challenge for internet banking providers in Malaysia. *Communications of the IBIMA, 5*, 133-142.

Ganesin, A., Supayah, L., & Ibrahim, J. (2016). An Overview of Cyber Security In Malaysia. *Kuwait Chapter of the Arabian Journal of Business and Management Review, 6*(4), 12.

Gani, A. B. D., & Fernando, Y. (2018). Concept and Practices of Cyber Supply Chain in Manufacturing Context *Encyclopedia of Information Science and Technology, Fourth Edition* (pp. 5306-5316): IGI Global.

Grönroos, C. (1984). A service quality model and its marketing implications. *European Journal of marketing*, *18*(4), 36-44.

Guraau, C. (2002). Online banking in transition economies: the implementation and development of online banking systems in Romania. *International journal of bank marketing, 20*(6), 285-296. https://doi.org/10.1108/02652320210446742.

Hamid, M. R. A., Amin, H., Lada, S., & Ahmad, N. (2007). A comparative analysis of Internet banking in Malaysia and Thailand. *Journal of Internet Business* (4).

International Monetary Fund, (2013). Retrieved from <International Monetary Fund 2013.pdf>

Jones, R. A., & Horowitz, B. (2012). A system-aware cyber security architecture. *Systems Engineering, 15*(2), 225-240.

Kim, D. Y. (2013). Relationship between supply chain integration and performance. *Operations management research, 6*(1-2), 74-90.

Ladhari, R., & Michaud, M. (2015). eWOM effects on hotel booking intentions, attitudes, trust, and website perceptions. *International Journal of Hospitality Management, 46,* 36-45.

Liao, H., & Chuang, A. (2004). A multilevel investigation of factors influencing employee service performance and customer outcomes. *Academy of Management journal, 47*(1), 41-58.

Mu, P. (2017). Local servers still at risk Cyber Security Malaysia. *New Sabah Times*, 7.

Muniandy, L., & Muniandy, B. (2012). State of cyber security and the factors governing its protection in Malaysia. *International Journal of Applied Science and Technology, 2*(4).

Obama, B. (2009). Obama's remarks on cyber-security. *New York Times*.

Pawar, K. S., Beltagui, A., & Riedel, J. C. (2009). The PSO triangle: designing product, service and organisation to create value. *International Journal of Operations & Production Management, 29*(5), 468-493.

Pikkarainen, T., Pikkarainen, K., Karjaluoto, H., & Pahnila, S. (2004). Consumer acceptance of online banking: an extension of the technology acceptance model. *Internet research, 14*(3), 224-235.

Ravichandran, T., Lertwongsatien, C., & Lertwongsatien, C. (2005). Effect of information systems resources and capabilities on firm performance: A resource-based perspective. *Journal of management information systems*, *21*(4), 237-276.

Rieback, M. R., Crispo, B., & Tanenbaum, A. S. (2006). The evolution of RFID security. *IEEE Pervasive Computing, 1,* 62-69.

Saffu, K., Walker, J. H., & Hinson, R. (2008). Strategic value and electronic commerce adoption among small and medium-sized enterprises in a transitional economy. *Journal of Business & Industrial Marketing, 23*(6), 395-404.

Santhanam, R., & Hartono, E. (2003). Issues in linking information technology capability to firm performance. *MIS quarterly*, 125-153.

Simpson, W. G., & Kohers, T. (2010). Journal of Business Ethics: JBE; Dordrecht. *35*(2), (Jan 2002), 97-109.

Siponen, M. T. (2005). An analysis of the traditional IS security approaches: implications for research and practice. *European Journal of Information Systems, 14*(3), 303-315.

Turban, E., King, D., Lee, J., Warkentin, M., & Chung, M. (2006). E-commerce: A managerial perspective. *Low Price Edition*, 180-183.

Wilding, N. (2016). Cyber resilience: How important is your reputation? How effective are your people. *Business Information Review, 33*(2), 94-99.

Williams, L. J., & Anderson, S. E. (1991). Job satisfaction and organizational commitment as predictors of organizational citizenship and in-role behaviors. Journal of management, *17*(3), 601-617.

Zikmund, W. G. (2003). The research process: an overview. *Business Research Methods, South Western: Cengage Learning.*