International Journal of Trend in Research and Development, Volume 6(2), ISSN: 2394-9333
www.ijtrd.com

Risk Management Framework for Prevent Cyber Crime in Jordan

[1]Hesham Al momani, [2]Diya Al-Jabali and [3]Heba Ahmad,
[1,2]Department of Industrial Engineering, Faculty of Engineering, The Hashemite University, Zarqa, Jordan
[3]Department of Business Administration, Faculty of Economics and Administrative Sciences , Yarmouk University, Irbid, Jordan

***Abstract*—**This main objective of this paper is to propose risk management framework for prevent the cyber crime in Jordan, the risk management is play an important role in cyber domains. Therefore by reviewing the related studies we identified the most critical success practices of risk management namely; identification , analysis and control. This paper present some of propositions which need examined in future and extend study.

Keywords*—Risk Management; Risk Management Practices; Cybe-Rcrime.*

I. INTRODUCTION

The rapid growth of information technology has become widespread in almost all levels of human activity. Private companies, government institutions, organizations and citizens use computers, computer networks and the Internet in an unprecedented way. The world is moving rapidly towards a connected digital society and, therefore, everyone needs to secure it in cyberspace [1]. Information security is in a rack of confidentiality, integrity and availability of data and services. Without an appropriate mechanism for information security, information technology can never reach its full potential as a serious tool in business and governance. The critical sectors of a modern state depend to a large extent on a complex network of interconnected computer systems. The proper functioning of these sectors is also important for national security. Any weakness in the computer systems that control these sectors can not only be devastating in terms of massive losses, but can threaten a nation. There is a need for a comprehensive approach to information security as an organizational priority to secure your digital assets. The identification of key success factors/ enabling factors for information security and their interrelation in an organization is useful for making strategic decisions in this regard.

Many organizations follow different security standards, such as ISO 27001: 2005, PCI-DSS, COBIT, etc. These laws and standards are also a driving force for organizations to take information security measures. Nothing as supreme security. Even after better efforts, the information security event can occur for several reasons. Organizations need to understand and mitigate risks. Risk management is the process that allows IT managers to balance the operational and financial costs of preventive measures for IT and data systems that support the functions of their organizations [2]. In Jordan, for example, there are some attempts at risk management in cybercrime, where special units have been established in the management and control of cybercrime.

To this end, one of the risk management goals is to identifying, analyzing and evaluating risk in the organization. Consequently, there is a need for more studies to examine the risk management in developing nations because despite the newness of risk management in such nations, it is perceived as a strategic approach that can develop and drive companies' values to higher performance levels. a few studies have been dedicated to studying risk management in cyber crime, indicating the lack of information and knowledge regarding it and the need for more studies in the area, specifically in Jordan [3]. This research therefore focuses on the examination of risk management to provide theoretical and practical contributions. On the whole, the present study is an attempt to provide deeper insight into risk management in cyber crime in Jordan. The structure of the paper is organized as follows: Section two provide the details about related studies. Section three explain the conceptual framework that would be proposed. Section four provide the conclusion.

II. LITERATURE REVIEW

[2] identified and developed a conceptual framework for the parameters for information security management. They classified parameters based on their powerful and reliance which facilitate information security management in the organization. also recommended parameters to which management have to pay more awareness. [3] found that risk management practices such as risk assessment and risk control are the most impacting constructs in the banks in Malaysia; whilst risk management and risk control have a good moderating of banks in Jordan.

[4] explored the relationship between the risk of cybercrime and the knowledge and use of crime prevention tools. The study found that people at increased risk of online fraud despite a careful understanding of the risks and knowledge of self-protective behavior in the Internet environment do not benefit from online prevention strategies. They concluded that the police agencies who designed cyber education have to provides guidance for the development of effective prevention programs based on the development of practical skills. [5] presented novel documentation on cyber risk worldwide for financial institutions by analyzing different types of cyber incidents (data breaches, fraud and business interruption) and identifying patterns using a variety of data sets. The other novel contribution described is a quantitative framework for assessing cyber risk for the financial sector.

[6] presented a potential analysis of the risk framework for Internet security in the organization described by three examples of future analyzes supported by cyber attacks. The first example is statistical analysis of the real database. The second is the analysis tool. The third analysis is the analysis of serial decisions to update the existing Internet security system software or to adopt a new system of survival for those who are trying to reach their path. The results are the loss distributions of cyber attacks, with or without some considered countermeasures to support risk management decisions based on past data and expected incidents. [1] Proposed an cyber risk mitigation tool and registry that assesses the potential for cyber attack; the basic premise is to monitor and qualify electronic risks directly based on the assets at risk and vulnerabilities of constantly updated programs. The tool produces risk scores that encourage enterprises to choose mitigation policies that can reduce premiums.

[7] analyzed the professional decision makers perceptions for cyber-security, with special emphasis on behavioral factors. The authors reported that the indicative availability, the

threshold of concern, the degree of anxiety and the confidence in the organizational capacity of each individual have a significant impact on the likelihood and potential impact of cyber attacks. They also discussed a possible explanation for the low demand for cyber-security insurance: the likelihood of a successful cyber attack tends to be exaggerated, while its financial impact is less than reality.

III. CONCEPTUAL FRAMEWORK

Based on the previous study, this research attempts to proposed a conceptual framework which discuses the impact of risk management on prevent cyber crim. Figure 1 present research conceptual framework.

A. Risk Management Practices

Risk management is considered is the most important variable to detect and prevent a cyber crime. These practices are discusses as a following;

1) Risk identification

According to [8], the risk management committee must identify, evaluate and respond to risks. Therefore, comprehensive and systematic risk identification processes are required to ensure that the risk assessment is correct. He also argued that drug identification is usually done only by a risk analyst during the interview of a member of the library or by the risk management committee. Actions at this stage include: identifying or engaging organizations, assessing the probability of each threat, evaluating the positive or negative impact of each threat, identifying procedures or controls to mitigate threats, estimating the costs and benefits of implementation controls . Exchange, acceptance or transfer of risk [3]. Thus, generally speaking, literature supports the first proposition proposed in this study, which states that;

P1:risk identification has a significantly influence on prevent cyber crime.

2) Risk analysis

Risk analysis is usually the most difficult task. Once completed, management must prioritize risks and respond to those who need immediate corrective action. Risk analysis as the process of identifying and measuring security risks and identifying appropriate areas requiring security measures [9]. Risk is assessed in several ways: probability, positive and negative, individual and collective, organizational unit, inherent, and residual software tools [5]. Thus, generally speaking, literature supports the second proposition proposed in this study, which states that;

P2:risk analysis has a significantly influence on prevent cyber crime.

3) Risk control

Risk control is defined as a process to reduce the amount of risk [10]. There should be adequate and clear policies and procedures. A study by [11], reported that adequate internal control samples include a system that can respond immediately to the background of changes in the environment, an adequate disaster emergency plan, internal audit reviews and backups. And data files of programs. Once applied, control mechanisms should be monitored continuously. Adverse events should be assessed, reported and answered in an agreed manner. [12] found that good internal controls could reduce mismanagement and attract confidence in the market. Thus, generally speaking, literature supports the third proposition proposed in this study, which states that;

P3:risk control has a significantly influence on prevent cyber crime.

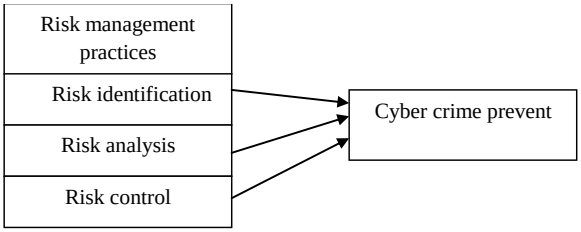

Figure 1: Research conceptual framework.

CONCLUSION

This review significantly contributes to the body of knowledge in terms of management of risk in cyber crime domain literature specifically in the context of Jordan by reviewing the risk management practices in various domains including the problems and challenges. Besides that, this research discusses the risk management practices such as risk identification, analysis and control. Also, this research proposed a conceptual framework and propositions that will need to examine in the future work.

References

[1] S. Shetty, M. McShane, L. Zhang, J. P. Kesan, C. A. Kamhoua, K. Kwiat, and L. L. Njilla, "Reducing informational disadvantages to improve cyber risk management," The Geneva Papers on Risk and Insurance-Issues and Practice, vol. 43, pp. 224-238, 2018.

[2] R. Shankar, M. Chander, and S. K. Jain, "Modeling of information security management parameters in Indian organizations using ISM and MICMAC approach," Journal of Modelling in Management, vol. 8, pp. 171-189, 2013/06/28 2013.

[3] R. A. Rahman, A. Alsmady, Z. Ibrahim, and A. D. Muhammad, "Risk management practices in Islamic banking institutions: A comparative study between Malaysia and Jordan," Journal of Applied Business Research, vol. 30, p. 1295, 2014.

[4] J. M. Drew and L. Farrell, "Online victimization risk and self-protective strategies: developing police-led cyber fraud prevention programs," Police Practice and Research, vol. 19, pp. 537-549, 2018/11/02 2018.

[5] A. Bouveret, Cyber risk for the financial sector: a framework for quantitative assessment: International Monetary Fund, 2018.

[6] M.-E. Paté-Cornell, M. Kuypers, M. Smith, and P. Keller, "Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies," Risk Analysis, vol. 38, pp. 226-241, 2018.

[7] G. de Smidt and W. Botzen, "Perceptions of corporate cyber risks and insurance decision-making," The Geneva Papers on Risk and Insurance-Issues and Practice, vol. 43, pp. 239-274, 2018.

[8] R. J. Chapman, "The effectiveness of working group risk identification and assessment techniques," International Journal of Project Management, vol. 16, pp. 333-343, 1998.

[9] Z. Ciechanowicz, "Risk analysis: requirements, conflicts and problems," Computers & Security, vol. 16, pp. 223-232, 1997.

[10] N. A. Doherty, Integrated risk management: Techniques and strategies for managing corporate risk: McGraw-Hill New York, 2000.

[11] T. Khan and H. Ahmed, "Risk Management: An Analysis of Issues in Islamic Financial Industry (Occasional Papers)," The Islamic Research and Teaching Institute (IRTI)2001.

[12] S. N. Makiyan, "Risk management and challenges in Islamic banks," Journal of Islamic Economics, Banking and Finance, vol. 4, pp. 45-54, 2008.