INFORMATION SECURITY ACCOUNTING & MANAGEMENT TO E-BUSINESS INTENTION: A REVIEW OF RESEARCH FINDINGS WITH EFFECTS OF THE JORDANIAN COMPANIES

AHMAD Y.A. BANI AHMAD

Irbid National University

Abstract - Information has turned out to be so inescapable in the day to day existence, that it is relatively irreplaceable. This is clear as information has progressed toward becoming center to the business operations of any enterprise. Information and communication technology (ICT) systems are vigorously depended upon to store, process and transmit this significant product. Because of its tremendous regard, data and related ICT resources have to be sufficiently secured. Such protection of information is usually alluded to as information security Accounting & management. Information security risks are a strategic issue which ought to be thoroughly addressed by all enterprises, public and private in nature. The government in Jordan not excluded. In any case, the Auditor-General of Jordan considers the larger part of information security practices within local government to be insufficient. The article piloted an enquiry of the empirical studies and models that related E-business intention, information securityAccounting & management and security risk. It essentially meant to prove the conceptualization estimation and examination of the distinct ideas. Following the analysis of literature, the findings indicated that information security Accounting & management; security risk and E-business intention significantly affects numerous Jordanian companies' procedures and customers. Likewise, the availability of security systems in any organization shall work in speeding up the concerned employees to evaluate their organization systems, supported with to Managers' approval and recommendations to acquire extensive variety of security.

Keywords - Information Security Accounting & Management, Intention, ICT, Risk, Jordan

I. INTRODUCTION

In any contemporary enterprise, both public and private, information is apparently of basic significance to the accomplishment of the enterprise and therefore, its worth is tremendous. The utilization and processing of such important data is essentially becoming more reliant on Information and Communication Technology (ICT) systems (Whitman & Mattord, 2012). This is because of the quick pace at which innovation is developing and its inescapability in modern enterprises. In this way, ICT is a noteworthy contributor to the effective implementation of business processes in enterprises over the world (Ifinedo, 2012). Therefore, in light of the massive value of information, it is imperative to protect all information assets, comprising the systems that accommodate the information.

Governments in Jordan have recognized this reality and are seeking various avenues in an effort to optimize their utilization of ICT in order to permit effective service delivery to the local population (JNI, 2017). This is unquestionably the case for the government of Jordan. Considering the above stated, this paper aims to briefly explain the structure of the Jordan government, determine the status of the utilization of ICT within government and lastly, motivate why information security management should be a key concern to government.

Most exact and up-to-date business information outside and inside a traditional firm as regards Jordan; is viewed risky and may cause sensational loss once practiced within the common use of banking services presented via internet. Without security system, such transactions may cause mistakes which could hardly been resolved. The Information Securing business is a burden as to the IT department and other staff of concern (Alabed & Hanandeh, 2013).

The Jordanian market is little and moderately poor. Numerous regional nations have bigger populaces and bigger economies. The Jordanian economy is on the whole involved MSMEs. MSMEs represent almost 99.6% of all registered firms (outside the agricultural part) (HDR, 2016). Most MSMEs are possessed and managed by the same individual. A large portion of these ventures, at the start up phase, were composed of only the owner. Currently, 76% of them have at least two employees (HDR, 2016).

II. LITERATURE REVIEW

Over the previous few years, telecommunication regulators have been approached by market players expecting regulators to be progressively involved in ICT security issues. Network and information security have always been important in telecom regulation, but the importance of security changes character with surfacing technologies. Security related to current communication systems, including Internet, are broader than security issues when telephony was the most dominant service. Current information and communication technologies raise a large range of questions for the reason that Internet is a more open environment than earlier communication systems; wireless communication likewise increases new security problems; and networks and services are

increasingly international, constituting new security issues (JNI, 2017).

To enable better ICT intersection with the economy and convergence across media will require that the Jordanian national ICT system (infrastructure and standards) be seen as secure. Investors, operators and users will only depend on ICT if it is perceived and demonstrated as secure. TRC and the GoJ should consider adopting national standards for ICT security, which can be adopted and executed by companies and operators depending on the standard of service which they will implement. This will necessitate that the GoJ and the TRC communicate the requisite of security to the operators and users to raise their awareness and to simplify improved ICT use in commercial and social transactions.

They advocate that, in order to make them significant to developing nations, it is imperative to enlarge these models to comprise factors that might reflect these nations' specific characteristics such as security. The variances that happen in different economic contexts, as well as the lack of rigorous research studies in the developing world, limit the general understanding of e-business productive execution among companies in nation like Jordan. Hence, rigorous research is required to improve our understanding of what factors might influence the adoption intention of e-business in a developing-economy context (Kumar Sharma & Madhumohan Govindaluri, 2014). Accordingly, the research work on security management system influencing factors in this study will be mentioned to from this region (the Middle East), particularly in Jordan as a prime focus.

To conclude Kang et.al, proposed a better emphasis on strategies and systems which protect security and privacy without reliant much on security practices of users. By criticizing the device centric ICT security approaches and the need to acquire knowledge on how to use and manage diverse set of security policies as per each device, Montero et al. (2015) recommended an access network level security policy model in their work. Thus, they claim that users would not be forced to learn how to use and manage a numerous set of security applications, given the increasing number of user terminals such as tablets, notebooks, smartphones, smart TVs, desktop computers and game consoles that a regular user possess. Nurkhin and Arief (2015), stated that perceived mobility value, social interaction, prior experience and perceived usefulness have impact on the user acceptance of technology. On the other hand, Shropshire, Warkentin, and Sharma (2015) studied the personality constructs that are effective in security software adoption. Their suppositions point the constructs influencing security software adoption is different than that of in regular software adoption. All the above mentioned studies specify the requirement for additional researches since results may offer valuable perceptions to policy makers in common. Therefore, we use above backdrop to include security related factors comprising information security Accounting & management system, E-business intention, security risk as intermediating factors in the study. To the best of our knowledge these factors have not been utilized in our context in the literature yet Especially in Jordan.

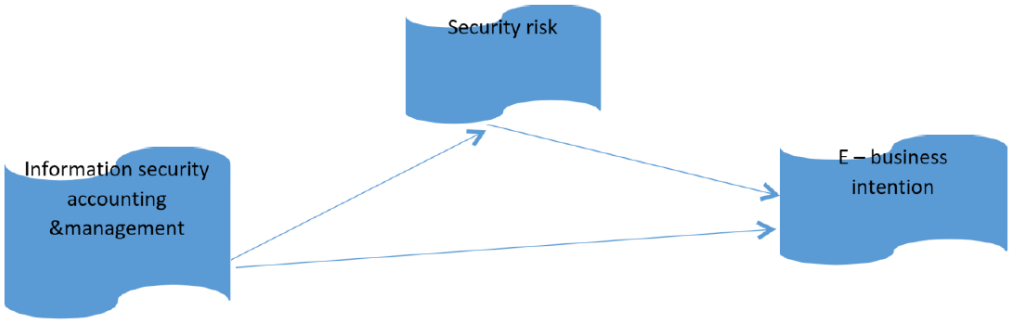

Figure 1: Conceptualization Framework

III. CONCLUSION

The non-existence of effects to information security Accounting & management system on E-Business intention, which is derived from the growing number of violations on international level, advance a point of impossibility to achieve 100% fulfillment. Those in charge should pursue numerous security procedures and approaches to maintain adequate security as to E-business intention. Employing high standards of security systems shall allow employees and customers to interact with the system at minimum limit of risk. For that reason, high level of security system may guarantee high level of productivity. And managers should emphasis on installing more security methods and procedures to warrant that employees will view better secure system. Form psychological point of view especially the number of internal attacks will be reduced as soon as employees perceive that their organizations deploy various security systems.

Finally, this article recommends future studies to carry out assessments by issuing out questionnaires amongst all companies such as (banks, telecommunications, computer companies, hotels ..... and so forth) in Jordan, to determine the effect of the study variables on the E-Business intention. This will have momentous implications to managers and the

resolution of the issues they encounter in the sectors, and very poor studies about information security Accounting & management and security risk in Jordan.

REFERENCES

[1] Alabed, S., & Hanandeh, R. (2013). The Impact of Implementing Information Security Management Systems on E-Business Firms: Case Study in Jordanian Banking Sector: Middle East University.

[2] HDR. (2016). Briefing note for countries on the 2016 Human Development Report. from http://hdr.undp.org/sites/all/themes/hdr_theme/country-notes/JOR.pdf

[3] Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83-95.

[4] JNI, C. (2017). Jordan National Information and Communications Technology Strategy 2013-2017. from http://trc.gov.jo/

[5] Kumar Sharma, S., & Madhumohan Govindaluri, S. (2014). Internet banking adoption in India: structural equation modeling approach. Journal of Indian Business Research, 6(2), 155-169.

[6] Montero, D., Yannuzzi, M., Shaw, A., Jacquin, L., Pastor, A., Serral-Gracia, R., . . . Sassu, R. (2015). Virtualized security at the network edge: A user-centric approach. IEEE Communications Magazine, 53(4), 176-186.

[7] Nurkhin, A., & Arief, S. (2015). The Determinant Of Student's Intention To Use Mobile Learning. PEOPLE: International Journal of Social Sciences, 1(1).

[8] Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. Computers & Security, 49, 177-191.

[9] Whitman, M., & Mattord, H. (2012). Hands-on information security lab manual: Cengage Learning.

★★★