Implementing Factors of Information Security in Governmental Organizations of Jordan

Ibrahim Obeidat
Prince Al-Hussein Bin Abdullah II Faculty of Information Technology
Hashemite University
Zarqa, Jordan
imsobeidat@hu.edu.jo

Ala Mughaid
Prince Al-Hussein Bin Abdullah II Faculty of Information Technology
Hashemite University
Zarqa, Jordan
Ala.mughaid@hu.edu.jo

***Abstract*— To maintain the integrity of information technology in governmental organizations, efficacious success factors in information security must be applied. Upon broad assessment and screening on the factors that influence information security, no permutation to successful assessment was reached. In addition, the influence of such factors has yet to be evaluated across the stages of assessment. This research's objective is the discovery of successful implementation of information security factors.**

Keywords- Information security; Success factors; Governmental Organizations.

I. INTRODUCTION

Today's society is data-driven. Collecting data from people, actions, algorithms, and the web has resulted in large data stores, and accommodating all this data has become a major challenge. 'Big data' tends to grow exponentially each year [14]. How secure is confidential information when people are not actually in their offices using a desktop computer, or when they are using a laptop computer on a network set up by a network administrator, When people take advantage of networking to use cloud computing services or to access e-mail on their own documents, they may accidentally risk the loss and/or disclosure of sensitive data and confidential client information. Organizations must pay more attention to data security and use protection tools to help secure their sensitive data and the confidential client information. Weak security systems used by the organizations may lead to data breaches and theft, resulting in major data losses and loss of customer's confidence in their service provider. The hierarchal structure of current organizations has placed more of emphasis on reinforcing possible breaches on an individual level due to the fact that Organizations depend more and more on computers and that computing control has been brought down to the individual desktop. Hence, realizing the importance of the type of environment people work in. More employees are interacting with technology to commence their daily tasks, and employees have established a greater threat because they have direct access to an organization's assets [5]. Also, information that is generated and stored on their individual desktop must remain confidential to the concerning party, this is because insufficient protection of confidential information may result in destruction, delay or disclosure to an illegal party [15]. Conventional computer systems may be desirable, but conventional security mechanisms are not sufficient against unauthorized access in cloud systems [7]. Network systems have provided many advantages to organizations, essentially providing a means of access to facilities and resources from any computer, anytime, anywhere, bringing about a technological revolution. However, organizations need to give more attention and consideration to their system security and need to guarantee that unauthorized individuals cannot access their information. A standout amongst the most undesirable circumstances to happen in systems is the unapproved access. This sort of access might be cultivated by an organization's official, or an unofficial intruder, or both. Such access may significantly harm the organization's notoriety by taking its imperative information, which favors adversely the organization's business dealings and diminishes its client's trust.

A number of risks and threats exist in the operational environment of computers and networks, particularly where they can become exposed to security breaches. There could be various reasons for the vulnerability, including an incorrect installation of systems, incorrect usage or malicious software.

In general, information shared among two or more computers over a network, may be exposed to the risk of intrusion. There are four ways of intrusion that can negatively affect the system [24]:

- Interception: An unwanted entity between the transmitter and the receiver steals the information.
- Interruption: Any unwanted entity between the conversations of two nodes stops the message and prevents it from being passed to the destination.
- Modification: An unwanted entity at the middle of a conversation of two nodes changes the sender's

 ISBN: 978-1-61208-685-9

messages, modifying their information before forwarding them to the receiver.

- Fabrication: A type of lie; here, one party is fabricated, and the other participants on the network are unaware that the messages are not from a valid participant.

Computer networks make it easier for organizations to distribute their business worldwide at a low cost. The Internet in particular increases the trading operations where organizations are targeting billions of customers. The open nature of the Internet makes it easy for people to access services from all over the world by using their own devices. Companies have developed and implemented easy access applications to provide their services over the Internet.

II. LITERATUE REVIEW

Studies on the factors affecting risk assessment practice and information security are light and there is a lack of experimental research in the area of security risk management [1]. Therefore, a need to consult a literature on factors affecting information security which helps us to identify a set of factors that may potentially affect the successful undertaking of information security risk assessment practices in organizations. These are listed in Table 1[4].

TABLE 1 SECURITY FACTORS

Critical Success Factors	Reference Discipline
Management support	Risk assessment Risk management Information security
User security awareness	Risk assessment Risk management Information security
Technical experts	Risk assessment Risk management Information security
Alignment with organization's objectives	Risk assessment Risk management Information security
Funding	Risk assessment Risk management Information security

"Information security relates to an array of actions designed to protect information and information systems" [4]. However, in statistics protection does not consist of only the information itself but also the entire infrastructure that enables its use, it covers hardware, software programs, threats, physical protection, and human factors, where each of these components has its own features. Consequently, information security plays a major role in the internet age of technology. Given that the number of organization security breaches is increasing daily, and the more available the information, the greater the dangers, it is expected that security will need to be tightened [17].

Because of the quantity of personnel, packages, and structures increases in the organizations, the control of the groups information becomes more difficult and therefore vulnerability potential propagates. Considering preferable practice of hardware and software program, notwithstanding, encouraging and empowering worker conduct, the organizations must make utilization of records and protection regulations. Data security coverage is a mixture of principles, rules, methodologies, strategies, and equipment installed to protect the business enterprise from threats. These guidelines also help agencies to become aware of its facts property and define the company mindset to these statistics belongings [16].

The authors of [3][10][19][26] agree that established standards, together with the worldwide widespread ISO 27002, are an excellent starting point for shaping the statistics safety policy to improve statistics safety in a company/business. ISO 27002 provides some recommendations associated with successful implementation of facts protection and is particularly supposed to help management to make decisions and then pass the important actions to those in management positions. ISO 27002 deals with:

- Security policy, objectives, and activities that properly reflect business objectives,
- Clear management commitment and support,
- Proper distribution and guidance on security policy to all employees and contractors,
- Effective 'marketing' of security to employees (including managers),
- Provision of adequate education and training,
- A sound understanding of security risk analysis, risk management, and security requirements,
- An approach to security implementation which is consistent with the organization's own culture,
- A balanced and comprehensive measurement system to evaluate the performance of information security,
- Management and feedback suggestions for improvement.

The authors of [2][16][20][21] quantify the causes and consequences of threats to information tackled by organizations. The following threats have been acknowledged by their researches:

1. Outside threats: computer viruses; herbal catastrophe; junk emails and hacking incidents.
2. Internal threats: set up or use of unauthorized hardware, peripherals; abuse of computer to get admission to controls; physical robbery of hardware or software program; human mistake; damage with the aid of an aggravated worker; use of employer resources for prohibited communications or sports

 ISBN: 978-1-61208-685-9

(porn browsing, electronic mail harassment) and installation or use of unauthorized software programs.

III. METHODOLOGY

The aim of this research is to evaluate the effect of the different information security factors implementation on governmental organizations. This research used the exploratory method by using a semi-structured qualitative method for collecting data and the grounded theory to get the results. The Data was categorized by defining patterns or topics and organizing them to derive meaning. This research was conducted in Jordan, for several governmental organizations. The research will depend on table 1 on designing the interview. There are more than 60 governmental organizations in Jordan , we used the semi-structured method to interview the selected samples , the samples consists of a mixture of Information technology and Information Security experts, in which they representing most of the governmental organizations in Jordan, we spent from forty minutes to one hour interviewing the population of the research, most of the expert samples were highly educated in IT, and most of them have more than three years' experience in their work, the semi-structures questioner was chosen in such a way to encourage the Population to explore their experience in their job as an Information Security Experts to grasp the success factors and the actions taken to secure the information. The selected sample is related to the in-depth nature of the qualitative approach used by author [30]. Reliability was addressed by a clear visualization of the research variables by means of multiple coders and case study procedure [22]. The questioners were clearly defined and have a summary of all the factors before given to the interviewees. The interview was conducted at the interviewee's convenient time.

IV. RESEARCH DISCUSSION AND FINDINGS

The success of the information security factors derived from the results are discussed below:

A. User Security Awarness and Training

The majority of the interviewees conceded to the organizations security. They imagined that the security can be accomplished by expanding the awareness and training. Some even admitted that awareness was next to nothing in their organization, and that the employees thought that the sole measure of security to maintain integrity was by using the username and password. Thus expanding, the awareness can be implemented through training employees in order to establish a sense of information security amongst them. The interviewees have requested the need of proceedings with preparations and plans to achieve execution of data security approaches. Author [8] Claims that organizations need to have continuing education and training plans to accomplish the essential outcome from the implementation of information security policies.

The 2002 security awareness index report mentioned by author [12] concluded that organizations all over the world are failing to make their employees aware of the security problems and concerns. The interviewees concluded that the majority of the security incidents in their organizations came out from their own employees identified as insider threat damage, this approves what author [23] finds, that employees are the biggest threat to information security. Other interviewees said that the outsider attacks come only from viruses and spam. Besides which, the interviewees do not face any real attack, but the viruses came from their employees when the employees themselves opened spam email or attached files. "The human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption, and secure access devices, and it is money a waste, because none of these measures address the weakest link in the security chain", where humans are the weakest link in the security chain [25]. So, if the security fails, that will weaken any organization. The interviewees also commented on some of the employee behavior claiming that some of them leave their computers on, other employees write the username and password on a small sheet near the computer and this will break the confidential to unauthorized people. That's why the research recommend doing a continuous course in training and awareness to all levels in the organization.

B. Management Support

Management commitment was essential in implementing the factors of information security, it was reflecting in assigning IT managers in the organizations' department to identify the importance of security in their organizations. A successful implementation of information security factors need very qualified staff. The Management tends not to start any procedure to guarantee the security of organizations because naturally they feel that the IT department is responsible for selecting the correct technologies, installing the essential software tools, keeping the technology in the organization and protect the organization's information [29]. That is what our interviewees confirmed; they said our management does not know everything we have to explain and convince them about the importance of the security of the organization and keep the IT department updated to keep the organization information secure. One of the interviewees said we cannot do anything without their permission; they have to give us support in implementing the security factors. Another expert said if the management does not understand our need to information security, whatever we do to prevent attacks and keep our information safe will fail. Hone et al. [18] clarify that the performance and the behavior of employees towards information security will be more coherent with secure behavior if the top management shows concern about the organization security. Thus it is recommended that the security procedures is set by the attitudes of those at the topmost of the organization [27]. Management will not support the information security except if they can see that it

 ISBN: 978-1-61208-685-9

supports the organization's important business purpose [28]. Hereafter they must be persuaded of the importance of information security before they will run enough budget, and act to apply the information security policy [9].

C. Funding

All expert interviewees agreed upon that the budget is the major concern that affects the successful implementation of information security; the budget is needed to buy the software tools for identifying the vulnerabilities and recommended controls, so funding must be sufficient because without enough money organizations cannot be secured. Hinde [27] defines budget as the financial facility which firstly wisely estimates the costs and secondly measures the access required to the resources to reach a successful implementation of information security. Budgets generally depend on the manner in which individuals' investments translate to outcomes, but the impact of security investment often depends not only on the investor's own decisions but also on the decisions of others [26]. One of the experts said that the vendors of security tools do not mention that after a while these tools must be updated to meet the new threats and attacks so without sufficient money our system organization will be vulnerable to the new attacks. It was, therefore, suggested that if the Organizations does not have the appropriate software tools or hardware that will lead to difficulties in control some security concerns like access control tools, assisting the employees to apply some security principles such as changing the password regularly or logoff after finishing their work. Another interviewee said that if they do not have the proper resources that may lead to lack of implantation of information security factors.

D. Alignment With the Organization's Objectives and Polices

Information security policy is a set of arrangements set by organizations' to guarantee that all data innovation clients' inside the space of the organization or its subsystem comply with rules and plans related to the security of digital information at any point inside the organizations' of the specialist. Each organization should ensure and control its information, moreover, it ought to be conveyed both inside and outside the organization's boundaries. This may cruel that data may need to be scrambled, authorized through a third party or an establishment and may have confinement set on its dissemination with reference to a classification framework laid out within the data security approach. The information security policy may be a plan identifying the organization's crucial resources with detail explanation with what is worthy, unsatisfactory and sensible behavior for the employee to ensure the security of data [13]. There is no question that the selection of good information security policy is the introductory degree that must be in place to play down the threat unsatisfactory utilize any of the organizations' data assets.

The interviewees said if we have a good information policy, compelling execution of this policy, acknowledgment from the employees, adhere to our rules and not try to control them, then that will positively affect the organization's performance and security. The participators mentioned that the organization's policy ought to be clear, understood by the employees, and it should be updated regularly.

IV. FINDINGS

Organizations ordinary do nothing in terms of security as long as nothing goes off-base but when things do go off-base they all of a sudden pay consideration and part of action is required to recover from the attack or the threat they face, indeed in spite of the fact some of the full-time recovery is inconceivable [11]. The observational findings developed from the interviewees affirm the significance of key basic information security factors mentioned in Table 1. Another new factor was found to be important which is using a suitable software tool. The important part of the management plays a recognized role in finding the suitable resources and managing the necessary policies and strategies, the management should provide essential funds and the right resources to guarantee that the controls are implemented, and this finding is balanced with author [6] which says that the management commitment in all levels is vital to guarantee the implementation of information security factors.

V. CONCLUSION AND FUTURE WORK

In this research a set of factors were illustrated that applies a great influence on different phases of the organizations' security. In spite of the fact that these factors are used in the existing literature. But their pertinence in the association of organization security has not been observationally discussed. Also, a new factor which is utilizing appropriate software tools was recognized, in order to facilitate information security in the governmental organizations. The foremost commitment to this paper, is fortifying the informative ability factors drawn from the existing literature, to satisfactory describe the success factors affecting the governmental organization in Jordan.

The findings were of great importance to the governmental organization in Jordan as well as in the organizations in the world, to realize compelling information security, achieve security in the organizations and to decrease the attacks and breaches. The paper recommended to follow-up studies, utilizing different distinctive strategies or diverse instruments. Finally this study is not without shortcoming, first, only five organizations were investigated and hence future work, must focus on multiple organizations. Second, we believe that the findings ought to be compared with non-governmental organizations, in order to study the influence of these factors on the information security of these non-governmental organizations.

 ISBN: 978-1-61208-685-9

REFERENCES

[1] A. Kotulic, and J. Clark, "Why there aren't more information security research studies" Vol.41,No.5,pp 597-607 ,2004.

[2] B. Lampson, " Computer Security in the Real World, Principles of Computer Systems" IEEE Computer Society,Vol. 1, pp. 37-48,2004.

[3] C. Pfleeger, and S. Pfleeger, " Security in computing" Prentice Hall, N.J., 2017.

[4] C. Richard, " AusCert Australian computer crime & security survey , Sustaining operational resiliency A process improvement approach to security management" Software Engineering Institute, Carnegie Mellon University, 2006.

[5] E. Madigan et al. " The cost of Non-Compliance-When Policies Fail" Proceedings of the32nd annual ACM SIGUCCS conference on User services, pp. 47 – 51, USA,2004.

[6] F. Katz, "The Effect of a University Information Security Survey on Instruction Methods in Information Security"ACM, USA , 2005.

[7] F. Bjorck, " Implementing Information Security Management Systems " Eigth Annual Working Conference on Information Security Management & Small Systems Security, USA ,2001.

[8] G. Dhillon, "Managing and Controlling Computer Misuse", Vol. 7, No. 4, pp. 171- 175,1999.

[9] GAO, "Information security risk assessment:Practices of leading organizations",USA, 1999.

[10] H. Saini and A. Saini , "Security Mechanismsat different Levels in Cloud Infrastructure" , International Journal of Computer Applications (0975-8887)Volume 108 No. 2 December 2014.

[11] H. Smith, et al. " Risk management in information systems:problems and potential" Communications of AIS (7) 2001.

[12] International Standards Organisation, ISO/IEC 27002," 2013.

[13] Information Systems Audit and Control Association, "Critical elements of information security program success"2005.

[14] J. Manyika, et al. " Big Data: The Next Frontier for Innovation, Competition, and Productivity" McKinsey Global Institute,2011.

[15] J. McCumber, " Assessing and managing security risk in IT systems: A structured methodology" Auerbach Publications, 2004.

[16] J. McKay, " Pitching the Policy: implementing IT Security Policy through Awareness" SANS Institute,

Management & Computer Security, Vol. 8, No. 1, pp. 31-41,2003.

[17] J. Brown, and S. Duguid, "The Social Life of Information" Boston, Harvard Business School Press,2002.

[18] K. Hone and J. Eloff , "What makes an Effective Information Security Policy", Network Security, Vol. 20, No. 6, pp. 14-16, 2002.

[19] L. Gordon and M. Loep, "Budgeting Process for Information Security Expenditures" Communications of the ACM, Vol. 49, No. 1, pp. 121-125,2006.

[20] M. Ernst and L. Young, "Global Information Security Survey " UK , 2013

[21] M. Al-Awadi, K. Renaud , " Success Factors In Information Security Implantation In Organization" IADIS International Conference e- Society,2007.

[22] M. Miles, and A. Huberman, " Qualitative Data Analysis" Sage Publications, Inc., 1994.

[23] N. Doherty and H. Fulford, "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis",Information Resources Management Journal, Vol. 18, No. 2, pp. 21-39, 2005.

[24] P. Fung and E. Jordan "Implementation of Information Security: A Knowledge-based Approach" The 6th Pacific Asia Conference on Information Systems,Japan, 2002.

[25] R. Anderson, and T. Moore, "The Economics of Information Security" Science USA, Vol. 314, No. 5799, pp. 610-613,2006.

[26] S. Canavan, " An Information Security Policy Development Guide for Large Companies"SANS Institute , Journal of Advanced Nursing, Uk ,Vol. 20, pp.716-721,2004.

[27] S. Hinde,"Security Surveys Spring Crop. Computers and Security", Vol. 21, No. 4, pp. 310-321,2002.

[28] S. Mikko "Information Management & Computer Security" A Conceptual Foundation for Organizational Information Security Awareness". Vol. 8, No. 8, pp. 31-44,2000.

[29] T. Tryfonas, et al. " Embedding Security Practices in Contemporary Information systems Development Approaches" Information Management & Computer Security, Vol. 9, No. 4, pp. 183-197. Siponen, M. T. 2001.

[30] T. Carr , " The Strengths and Weaknesses of Quantitative and Qualitative Research :What Method forNursing" Journal of Advanced Nursing, Vol.20,pp.716-721, 1994.

 ISBN: 978-1-61208-685-9