Information Assurance Practices in Saudi Arabian Organizations

Abdulaziz Alarifi(✉)

Compuer Science Department, Community College, King Saud University, Riyadh, Saudi Arabia
abdulazizalarifi@ksu.edu.sa

Abstract. While the Web, cell phone 'apps' and cloud computing put a world of information at our fingertips that information is under constant threat from cyber vandals and hackers. Although awareness of information threats is growing in the Western world, in places like Saudi Arabia, information security is very poor. Unlike Western pluralistic democracies, Saudi Arabia is a highly-censored country, with a patriarchal and tribal culture, which may influence its poor information security rating. This paper examines the level of Information Security (InfoSec) practices among the IT departments in organizations in Saudi Arabia, using an online survey, based on instruments produced by specialist organizations on information security such as the Malaysian Cyber Security Organization, the Excellence of Information Assurance Centre, and Alelm organization in Saudi Arabia. The survey attracted 124 respondents and the results indicated that information security in Saudi Arabian organizations is quite low. Several of the areas of weakness in InfoSec appear to be related to the level of censorship or the patriarchal and tribal nature of Saudi culture. This study has clearly indicated that information security in Saudi Arabia faces some serious risks from a range of threat types. There is a need to reduce the risks faced and provide good strategies for further protection from threats quickly. This study has proposed the InfoSec Cultural Adaptation Process model (InfoSec CAP) as a process to inform a culturally appropriate response to this challenge. The vision of this research was to provide a tool that would protect and enhance the InfoSec in Saudi Arabia in the short and long terms. This was provided in the Info-Sec CAP model. The use of the model will help to establish a strong information security practice and to provide a further information protection. It will also help embed the identified concepts in information security practice globally.

Keywords: Information security · Information assurance · Information systems · Information security management

1 Introduction

The World Wide Web, mobile computing, and Cloud Computing have changed the world, providing a wide range of information, anytime and anywhere [1]. However, the developments of such technologies also allows new techniques for abusers to misuse or destroy information [2]. These "cyber vandals" can illegally access or destroy online information using techniques such as malware programs (e.g. viruses, Trojans and worms), hacking or denial of service (DoS) attacks [3].

C. Stephanidis (Ed.): HCII 2015 Posters, Part II, CCIS 529, pp. 637–642, 2015.
DOI: 10.1007/978-3-319-21383-5_106

To overcome these threats, it is essential for both information providers and information users to have good information security practices, which can be defined as ensuring the availability, integrity and confidentiality of information [4–6]. However, before Information Security practices become routine, there must be an appropriate level of Information Security Awareness (ISA), which refers to a state in which information users are aware of the information risks and understand the power of both physical and non-physical information security [7, 8]. ISA has become one of the strongest lines of defense against ongoing information threats; it has been demonstrated that a high-level of ISA can reduce information risks and increase the efficiency of information security performance [7].

Although this is generally well-understood, some countries, particularly those which are highly-censored, such as Saudi Arabia, does not appear to have understood either the devastating risks of information security (InfoSec) threats or the importance of ISA. Indeed, Saudi Arabia has among the highest levels of information security risk [9]. This paper aims to understand the relationship between these high risk levels and InfoSec, specifically in the context of Saudi Arabia.

2 Methodology

While our understanding of InfoSec in Saudi Arabia is poor, the concept of InfoSec is well-defined in the literature and several excellent survey instruments exist for assessing InfoSec. Moreover, this study seeks to gather data from as large a sample of the Saudi Arabian organizations as possible, so a survey is an ideal data gathering technique [10, 11]. An online survey is particularly effective over long distances and is well-suited to Saudi culture because women in Saudi Arabia cannot speak to men who are not relatives. Consequently, an online survey can gather a large sample from organizations of both men and women in a short time without any ethical problems.

The survey questions were selected from instruments developed by the Cyber Security Organization in Malaysia the Excellence of Information Assurance Centre and Alelm organization in Saudi Arabia. All of the survey questions from either survey were included unless they would have been inappropriate for the Saudi culture.

The questions in this research were semi-closed ended question that combine the advantages of closed-ended questions and open-ended questions. The survey was translated into the Arabic language because the participants are all from Saudi Arabia. The initial survey was subjected to pilot testing by Saudis who were fluent English speakers to ensure both the validity of the questions and the accuracy of their translation into Arabic. Pilot test participants strongly recommended making all questions optional as they believed that many Saudis would simply stop answering the questions if they encountered a compulsory question that they did not want to answer. The survey questions were then uploaded to Survey Monkey with all questions being optional.

To ensure the high response rate, the researcher distributed an online link to the survey using popular Saudi organizations educational and business websites and IT departments staff emails. This worked well, resulting in 124 responses.

3 Results

Although there were 124 organizational participants from Saudi Arabia in this study, responses in this paper focuses on InfoSec practices in organizations.

This section discusses information assurance tools and measures in the organizations including in two-factor authentications, password practices, firewall system, anti-viruses software and Information security training for employees.

As depicted in Table 1, 82 of the 124 organizations have not implemented two-factor authentication such as smart cards, biometric or one time passwords, whereas the remaining one-third already implements two-factor authentication. Pairing of two basic authentication approaches is very well established among many organizations. However, cautioned that "although use of two-factor authentication increases the overall security by additional layer of complexity, it is important to realize that these systems are not infallible" [12].

Table 1. Implementation of two-factor authentication in organizations

Does your organization implement two factor authentication in your organization (i.e. smart-card, biometric, one time password… etc.)			
		Frequency	Percent
Valid	Yes	42	33.9 %
	No	82	66.1 %
	Total	124	100 %

Data from Table 2 revealed that 31.5 % of the organizations have poor security measures with respect to password setting on the assessment of their respondent-representatives to the present study. Meanwhile, slightly over one-fifth of the organizations have very poor procedures in setting passwords. Only 8.1 % of the organizations have very good password measures, whereas 16.9 % have good password setting security processes. On the other hand, 17.7 % chose to stay neutral regarding the issue and 4 % of the respondents reported that password setting is not practiced in their organizations. It may be observed from the framing of the item that it was the practice,

Table 2. Passwords practices in organizations

How secure is your organization process/practice in setting passwords?							
	Not Exist	Very Poor	Poor	Neutral	Good	Very Good	Total
Frequency	5	27	39	22	21	10	124
Percent	4 %	21.8 %	31.5 %	17.7 %	16.9 %	8.1 %	100 %

not the policy, which was being evaluated. As posited in [13], "password mechanisms and their users form a socio-technical system, whose effectiveness relies strongly on users' willingness to make the extra effort that security conscious behavior requires".

Table 3 revealed that most of the respondents 29.8 % stood on neutral ground with respect to the firewall systems installed in their organizations. About 33.1 % of the organizations reported that their firewall systems are good or very good, whereas 34.7 % of the organizations have poor or very poor firewall systems. Three (2.4 %) organizations do not have security firewall systems. Firewalls are one of the most crucial elements in InfoSec. The secret to the success of firewalls is the formulation and implementation of filtering rules which protect the system from unauthorized access [14].

Table 3. Firewall system in organizations

How secure is your organization Firewall system to protect against undesired access to organization servers from outside the organization?							
	Not Exist	Very Poor	Poor	Neutral	Good	Very Good	Total
Frequency	3	14	29	37	25	16	124
Percent	2.4 %	11.3 %	23.4 %	29.8 %	20.2 %	12.9 %	100 %

Table 4 revealed that 43.5 % of the anti-virus software used by the organizations have good or very good performance ratings. Meanwhile 34.7 % of the organizations adopted a neutral stance regarding the anti-virus software issue. On the other hand, 19.4 % of the organizations indicated poor or very poor ratings for their anti-virus software. Anti-virus software is a crucial element of InfoSec because it serves as a solid line of defense capable of detecting and removing viruses before it causes significant harm to the system and the data stored in it [15].

Table 4. The strength of anti-virus software in organizations

How strong is your organization anti-virus software?							
	Not Exist	Very Poor	Poor	Neutral	Good	Very Good	Total
Frequency	3	8	16	43	36	18	124
Percent	2.4 %	6.5 %	12.9 %	34.7 %	29 %	14.5 %	100 %

Table 5 indicated that majority of organizations (70.2 %) have not offered special InfoSec training to employees. On the other hand, 29.8 % reported offering special InfoSec training. Adequate InfoSec training for all employees is required as per InfoSec standards. Common training areas include information security awareness, asset classification and control, responding to security-related events, web access and messaging, user access control and responsibilities, legal compliance, as well as business continuity awareness and procedures [16].

Table 5. InfoSec training offered to employees in organizations

Does your organization offer special information security training to employees?			
		Frequency	Percent
Valid	Yes	37	29.8 %
	No	87	70.2 %
	Total	124	100 %

4 Conclusions and Future Research

This paper has suggested that the level of attacks may be due to a lack of Information Security (InfoSec) practices among the Saudi organizations. A survey of 124 organizations in Saudi Arabia has indicated that InfoSec practices are in fact very low and that a number of information security risks may be related to Saudi awareness or culture.

The paper has indicated that a problem exists within the IT practices of many Saudi organizations. The next phase of this research will provide appropriate solutions for the existed weaknesses and recommendation to increase the InfoSec awareness and practices in organizations in Saudi Arabia. This study will proposed the InfoSec Cultural Adaptation Process model (InfoSec CAP) as a process to inform a culturally appropriate response to this challenge.

References

1. Afyouni, H.: Database Security and Auditing: Protecting Data Integrity and Accessibility. Thomson Course, Canada (2006)
2. Bragg, R., Ousley, M., Strassberg, K.: Network Security: The Complete Reference. Coral Ventura, Newbury Park (2004)
3. Easttom, C.: Computer Security Fundamentals. Pearson Prentice Hall, New York (2006)
4. Turban, E., Wetherbe, J., McLean, E.: Information Security Technology for Management: Improving Quality and Productivity, 3rd edn. Wiley, Hoboken (1996)
5. Stallings, W., Brown, L.: Computer Security Principles and Practice. Pearson Education, New York (2008)
6. Whitman, M., Mattord, H.: Management of Information Security. Thomson Course Technology, Canada (2008)
7. Siponen, M.: A conceptual foundation for organizational: information security awareness. Inf. Manage. Comput. Secur. **8**, 31–41 (2000)
8. Kruger, H., Drvein, L., Steyn, T.: A vocabulary test to assess information security awareness. Inf. Manage. Comput. Secur. **18**, 316–327 (2010)
9. Kaspersky Security Bulletin (2011). http://www.kaspersky.com/reading_room?chapter=207716858 Accessed 3 January 2012
10. Creswell, J.: Research design: Qualitative, Quantitative, and Mixed Method Approaches. Sage Publications, California (2003)

11. Hancock, D., Algozzine, B.: Doing Case Study Research. Teachers College Press, New York (2006)
12. Furnell, S., Katsikas, S., Lopez, J., Patel, A. (eds.): Securing Information and Communication Systems: Principles, Technologies, and Applications. Artech House, Norwood (2008)
13. Weirich, D., Sasse, M.A.: Pretty good persuasion: a first step towards effective password security in the real world. In: Raskin, V., Greenwald, S.J., Timmerman, B., Kienzle, D.M. (eds.) NSPW (National Secuirty Paradigms Workshop) Proceedings of the 2001 Workshop on New Security Paradigms. Association for Computing Machinery (ACM), New York (2001). Cloudcroft, New Mexico, 10–13 September 2001
14. Al-Shaer, E.S., Hamed, H.H.: Modeling and management of firewall policies. IEEE Trans. Netw. Serv. Manage. **1**, 2–10 (2004)
15. Ferguson, B.: Network + Fast Pass. SYBEX, Alameda (2005)
16. Calder, A.: Information security training. In: Reuvid, J. (ed.) The Secure Online Business Handbook: A Practical Guide to Risk Management and Business Continuity. Kogan Page, Philadelphia (2006)