ARC '16

مؤتمر مؤسسة قطر
السنوي للبحوث
QATAR FOUNDATION
ANNUAL RESEARCH
CONFERENCE

Towards World-class
Research and Innovation

مؤسسة قطر
Qatar Foundation
لإطلاق قدرات الإنسان
Unlocking human potential

Information Communications Technology Pillar

http://dx.doi.org/10.5339/qfarc.2016.ICTPP2531

Enhancing Information Security Process in Organisations in Qatar

Aisha Khalid Al-Hamar

Qatar Foundation, QA

Email: akj_qtr@hotmail.com

Due to the universal use of technology and its pervasive connection to the world, organisations have become more exposed to frequent and various threats (Rotvold, 2008).Therefore, organisations today are giving more attention to information security as it has become a vital and challenging issue. Mackay (2013) noted that the significance of information security, particularly information security policies and awareness, is growing due to the increasing use of IT and computerization. Accordingly, information security presents a key role in the internet era of technology. Gordon & Loep (2006) stated that information security involves a group of actions intended to protect information and information systems. It involves software, hardware, physical security and human factors, where each element has its own features. Information security not only secures the organisation's security but the complete infrastructure that enables the information's use. Organisations are facing an increase in daily security breaches, especially information that is more accessible to the public as the threat becomes greater. Therefore security requirements need to be tightened.

Information security policies control employees' behavior as well as securing the use of hardware and software. Organisations benefit from implementing information security policies as it helps them to classify their information assets and define the importance of the information assets to the organisation (Canavan, 2003). Information security policy as a number of principles, regulations, methodologies, procedures and tools created to secure the organisation from threats. Boss and Kirsch (2007) stated that employees' compliance with information security polices has become an important socio-organizational resource. Information security policies are applied in organisations to provide the employees with guidelines to guarantee information security.

Herold (2010) expressed the importance for organisations to have constant training programmes and educational awareness to attain the required result from the implementation of an information security policy. Security experts' emphasise the importance of security awareness programmes and how they improve information security as a whole. Nevertheless, implementing security awareness in organisations is a challenging process as it requires actively

Cite this article as: Al-Hamar AK. (2016). Enhancing Information Security Process in Organisations in Qatar. Qatar Foundation Annual Research Conference Proceedings 2016: ICTPP2531 http://dx.doi.org/10.5339/qfarc.2016.ICTPP2531.

interacting with an audience that usually does not know the importance of information security (Manke, 2013). Organisations tend to use advanced security technologies and constantly train their security professionals, while paying little attention on enhancing the security awareness of employees and users. This makes employees and users the weakest link in any organization (Warkentin & Willison, 2009).

In the last ten years, the state of Qatar has witnessed remarkable growth and development of its civilization, having embraced information technology as a base for innovation and success. The country has perceived tremendous improvement in the sectors of health care, education and transport (Al-Malki, 2015). Information technology plays a strategic role in building the country's knowledge based economy. Due to the country's increasing use of internet and being connected to the global environment, Qatar needs to adequately address the global threats arising from the internet. The global role of Qatar in world politics has led Qatar to not just face the traditional threats from hackers, but more malicious performers such as terrorists, organized criminal networks and foreign government spying. Qatar has faced a lot of discomfort with some countries which try to breach the county's security. Qatar Computer Emergency Response Team (Q-CERT) who is responsible of addressing the state's Information Security needs stated "As Qatar's dependence on cyberspace grows, its resiliency and security become even more critical, and hence the needs for a comprehensive approach that addresses this need" (Q-CERT, 2015). Therefore Q-CERT established National Information Assurance policy (NIA), which is an information security policy designed to help both government and private sectors in Qatar, to protect their information and enhance their security. Nevertheless the NIA policy has not been implemented still in any organization in Qatar. This is due to the barriers and challenges of information security in Qatar such as culture and awareness, which make the implementation of information security policies a challenging approach.

As a result, the scope of this research is to investigate information security in Qatar. There are many solutions for information security, some are technical and others are non-technical, such as security policies and information security awareness. This research focusses on enhancing information security through non-technical solutions, in particular information security policy. The aim of this research is to enhance information security in organizations in Qatar by developing a comprehensive Information Security Management System (ISMS) that considers the country-specific and cultural factors of Qatar. ISMS is a combination of policies and frameworks which ensure information security management (Rouse, 2011). This information security management approach is unique to Qatar as it considers Qatar culture and country specific factors. Although there are a lot of international information security policies available, such as ISO27001 but this research shows that sometimes these do not address the security needs particular to the culture of the country. Therefore there was a need to define a unique ISMS approach for Qatar.

To accomplish the aim of this research the following objectives must be achieved.

1. To review literature on information security in general and in Qatar in particular.
2. To review international and local information security standards and policies.
3. To explore the NIA policy in Qatar and compare it with others in the region and internationally.
4. To define problems with implementing information security policies and NIA policy in particular in organisations in Qatar.
5. To provide recommendations for the new version of the NIA policy.
6. To assess the awareness of employees on information security.
7. To assess the information security process in organisations in Qatar.
8. To identify the factors which affect information security in Qatar including culture and country specific factors.
9. To propose an ISMS for Qatari organisations taking into consideration the above factors.
10. To define a process for organisations to maintain the ISMS.
11. To evaluate the effectiveness of the proposed ISMS.

To achieve the aim of this research, different research methodologies, strategies and data collection methods will be used, such as literature review, surveys, interviews and case study. The research undergoes three phases, currently the researcher has completed phase one of the research which analyses the field of information security and highlights the gaps in the literature that can be investigated further in this research. It also examines the country factors that affect information security and the implementation of such information security policies. While undertaking interviews with experts in the field of information technology, information security, culture and law, to identify the situation of Information Security in Qatar, and the factors which might affect the development of Information Security in Qatar including the cultural effect, legal and political issues. In the following two years, the researcher will complete phase two and three of the research. During phase two the researcher will measure the awareness of employees and their knowledge of information security and information security policies in particular. The finding will help the researcher in completing phase three which involves investigating further the NIA policy and a real implementation of ISMS in an organisation in Qatar, and analyses the main findings to finally providing recommendations for improving NIA policy.

In conclusion, the main contribution of this research is to investigate the NIA policy and the challenges facing its implementation, and then define an ISMS process for the policy to assist organisations in Qatar in implementing and maintaining the NIA policy. The research is valuable since it will perform the first real implementation of the NIA policy in an organisation in Qatar taking advantage of the internship the researcher had with ICT. The research will move the policy from paper-based form into a real ISMS system and oversees it in reality in one of the organizations.

Keywords

Information security, National Information Assurance policy, Information Security Management System, Security Awareness, Information Systems

References

Rotvold, G. (2008). How to Create a Security Culture in Your Organization. Available: http://content.arma.org/IMM/NovDec2008/How_to_Create_a_Security_Culture.aspx. Last accessed 1st Aug 2015.

Manke, S. (2013). The Habits of Highly Successful Security Awareness Programs: A Cross-Company Comparison. Available: http://www.securementem.com/wp-content/uploads/2013/07/Habits_white_paper.pdf. Last accessed 1st Aug 2015.

Al-Malki. (2015). Welcome to Doha, the pearl of the Gulf. Available: http://www.itma-congress-2015.com/Welcome_note_2.html. Last accessed 4th May 2015.

Rouse, M. (2011). Information security management system (ISMS). Available: http://searchsecurity.techtarget.in/definition/information-security-management-system-ISMS. Last accessed 22th Aug 2015.

Q-CERT. (2015). About Q-CERT. Available: http://www.qcert.org/about-q-cert. Last accessed 1st Aug 2015.

Warkentin, M., and Willison, R. (2009). “Behavioral and Policy Issues in Information Systems Security: The Insider Threat,” European Journal of Information Systems (18:2), pp. 101–105.

Mackay, M. (2013). AN EFFECTIVE METHOD FOR INFORMATION SECURITY AWARENESS RAISING INITIATIVES. International Journal of Computer Science & Information Technology. 5 (2), p 63–71.

Gordon, L. A. & Loep, M. P. (2006). Budgeting Process for Information Security Expenditures. Communications of the ACM. 49 (1), p 121–125.

Herold. R (2010). Managing an Information Security and Privacy Awareness and Training Program. New York: CRC Press.

Boss, S., & Kirsch, L. (2007). The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines. International Conference on Information Systems. unknown (unknown), p 9–12.

Canavan, S. (2003). An Information Security Policy Development Guide for Large Companies. SANS Institute.