MWAIS 2011 Proceedings

Midwest (MWAIS)

5-20-2011

Towards Developing A Framework for Managing an Information Security Policy in Healthcare Organizations

Alaa A. AlWabel
King Khaled University, a.a.wabel@hotmail.com

Abdulrahman A. Mirza
King Saud University, amirza@ksu.edu.sa

Towards Developing A Framework for Managing an Information Security Policy in Healthcare Organizations

Alaa A. AlWabel
King Khaled University
a.a.wabel@hotmail.com

Abdulrahman A. Mirza
King Saud University
amirza@ksu.edu.sa

ABSTRACT

In today's interconnected high-tech world, healthcare organizations are especially concerned with managing and securing health-related information. Threats exist from different sources, and breaches have undesirable impact on the healthcare organization. In order to enhance the organization's security, a precise and clear information security policy must be introduced and enforced. This is an important area of concern that should be addressed properly to successfully manage health organizations' security. This is a research-in-progress that examines the need for the adoption of standardized policies and regulations when it comes to dealing with the issue of information security in healthcare organizations. As an outcome of this research we hope to develop a simplified framework that can assist healthcare organizations in the implementation and management of an effective information security policy (ISP). The intended framework is expected to be of great benefit to the smaller healthcare organizations that may be lacking the necessary information security expertise. A study will be conducted on the status of information security within Saudi Arabian healthcare organizations in an effort to strengthen the recommendations of the proposed framework.

Keywords

Information Security Policy (ISP), Healthcare Management, Healthcare Organizations, Saudi Arabia.

INTRODUCTION

One of the most important and valuable assets to a healthcare organization is information. Thus, protecting this asset is required to ensure confidentiality, integrity, and availability. In order to receive treatment, people must provide healthcare organizations with sensitive information. Most patients expect such organizations to preserve the privacy and integrity of their information. Thus, healthcare organizations have a legal and ethical responsibility to protect sensitive information about their patients, care providers, contractors, vendors, and, any other individual or organization engaged in communications with such a healthcare provider (Copper, 2007).

The International Standards Organization (ISO) has pointed-out that small healthcare providers typically lack the necessary IT resources for managing information security; hence, it recommends that rigorous controls are put into place to appropriately protect health information (Rachel et. al., 2009). The US Department of Health and Human Services (HHS) has also highlighted the importance of ensuring the security and privacy of health information (Redspin, 2010). In 1996, the British Medical Association (BMA) issued a report entitled "A Security Policy Model for Clinical Information Systems;" the policy addressed the need to work on nine main principles in order to deal with health information security problems including access control, record opening, consent, notification, attribution, persistence, information flow, aggregation control, and, trusted computing base (Anderson, 1996). Healthcare Information and Management Systems Society (HIMSS) issued in 1997 the "Guidelines for Establishing Information Security Policies at Organization with Computer-based Patient Record Systems." It was recommended by the Working Group on Confidentiality, Privacy, and Security in order to encourage the creation of policies and mechanism to protect patient and care provider privacy and ensure information security. Among the important parts of the guidelines are "the principles" upon which the guidelines are based, including: information security philosophy, responsibility and accountability, ethical and legal rights, awareness and security training, monitoring and auditing, disaster recovery, and resumption plans (Copper, 2007).

Healthcare organizations in Saudi Arabia today are moving faster towards using IT systems to electronically record, share and store healthcare information in order to speed up their operations and reduce managerial and storage costs. Accordingly, the need for providing a secure environment to protect healthcare information has increased. Security challenges to these organizations come from a wide range of sources and may have undesirable impacts on their management facilities, business continuity, employee safety, and patient data privacy (SAHI, 2010). Additionally, there is a great shortage in qualified information security personnel in Saudi Arabia that adds to the difficulties of dealing with such important issues (Nabi, et. al., 2010).

Consequently, there is a significant need to create, implement, and enforce data security and confidentiality policies in Saudi Arabian healthcare organization as recommended by (Maghazil, 2004). As a result, this is an important area of concern that should be addressed properly to successfully manage health information security in Saudi Arabia.

AIM AND METHODOLOGY OF THIS STUDY

The goal of this research is to initially examine the status of information security policies in Saudi Arabian healthcare organizations; it also aims to discover the level to which such policies are adopted and implemented, and the level of success to which these policies are enforced. We eventually aim to develop a simplified framework that can be used to assist healthcare organizations in the proper implementation and management of an ISP. This proposed framework will include the necessary processes behind such implementation and management.

In order to accomplish our research aims, we plan to initially conduct an online survey that we target towards IT managers, information security officers, and/or, health informatics specialists belonging to Saudi healthcare organizations. This survey tool will be developed based on HIPPA and ISO guidelines with regard to information security. It will also be developed with the STOPE view as an assessment approach that includes consideration of Strategy, Technology, Organization, People, and Environment (Bakry, 2003).

In developing our ISP framework, we will also develop it in the same spirit of the STOPE methodology as we aim to concentrate on the following issues:

- Strategy: This includes the strategic national and organizational planning towards the adoption of information security practices and control mechanisms.
- Technology: The healthcare IT infrastructure at hand including electronic health records, systems backup, business continuity, disaster recovery, picture archiving, and other important IT infrastructure issues (Woburn, 2010).
- Organization: Important managerial issues specifically those dealing with the structure and functions of IT departments.
- People: The people within a healthcare organization that are concerned with the entry, management, and protection of healthcare information including healthcare practitioners, IT personnel, IT managers, and health informatics specialists.
- Environment: The environment concerned, including managerial behavior, legal and ethical behavior and rules, social influences, and country-specific regulations and standards.

CONCLUSION

Through this research project we hope to develop a clear picture of the current status of information security policies within healthcare organizations in Saudi Arabia; and, the level to which such ISPs are enforced and deemed to be effective. We also seek to develop a simplifies framework for the implementation and management of an ISP for healthcare organizations based on well-established standards and methodologies, with the ultimate goal of much improved information security processes and controls. We hope that results of this study can be of great use to healthcare organizations, especially those with a shortage in experienced information security personnel.

REFRENCES

1. Anderson, R.J (1996) A Security Policy Model for Clinical Information Systems, published by the British Medical Association, January 1996, retrieved from http://www.cl.cam.ac.uk/~rja14/Papers/oakpolicy.pdf.
2. Bakry, S.H. (2003) Development of security policies for private networks, International Journal of Network Management. Wiley, Vol. 13, Issue 1, pp 203-210.
3. Copper, T. (2007) Guidelines for Establishing Information Security Policies at Organizations with Computer-based Patient Record Systems, Healthcare Information and Management Systems Society, retrieved from http://www.himss.org/content/files/CPRIToolkit/version6/v6%20pdf/D38_CPRI_Guidelines-Information_Security_Policies.pdf

4. Maghazil, M. (2004) A comparative analysis of data security in computer-based and paper-based patient record systems from the perceptions of healthcare providers in major hospitals in Saudi Arabia, doctoral thesis, The George Washington University, retrieved at http://portal.acm.org/citation.cfm?id=997743.
5. Nabi, S., Mirza, A., and Alghathbar, K., ‘Information Assurance in Saudi Organizations,’ Jeju Island, South Korea, International Conference on Security Technologies (SECTECH’10), Jeju Island, South Korea, December, 13-15, 2010.
6. Redspin (2010) Trends in Healthcare IT: Understanding HITECH, the HIPAA Security Rule, and How to Safeguard Your Electronic Protected Health Information (EPHI), retrieved at http://www.redspin.com/docs/Redspin_WP_TrendsinHealthcareIT.pdf
7. Saudi Association for health Informatics (SAHI) (2010) Applied Health Informatics on Saudi E-health conference, Riyadh, Saudi Arabia, http://www.saudiehealth.org/.
8. Woburn (2010) Data Management Investments Top Healthcare’s IT Priorities Over the Next 12 Months, Healthcare Storage Virtualization (HSV) Company, retrieved at http://www.bridgeheadsoftware.com/pdf_news/BH_Corp_PR_BridgeHead-Announces-Research-Results.pdf.