International Conference on Control, Engineering & Information Technology (CEIT'13)
Proceedings Engineering & Technology - Vol.3, pp. 12-16, 2013

Toward Healthcare Information Security as a Service and a Security Blueprint

Chalee Vorakulpipat[#1], Siwaruk Siwamogsatham[#2], Asanee Kawtrakul[#3]

[#]*National Electronics and Computer Technology Center*
112 Thailand Science Park, Phahonyothin Road,
Klong 1, Klong Luang, Pathumthani 12120 Thailand
[1]chalee.vorakulpipat@nectec.or.th
[2]siwaruk.siwamogsatham@nectec.or.th
[3]asanee.kawtrakul@nectec.or.th

***Abstract*— In healthcare services, information security has become a vital focus. This is because personal data like patient's records are very sensitive regarding privacy issues and health information system is highly related to human safety. This paper aims to explore information security practices in several small-sized healthcare sectors. The analysis of the survey results could lead to the generation of a guideline for development of information security as a service and a security blueprint for small-sized hospitals based on three business factors: organizational structures, processes, and systems. The study suggests that a consulting service (for management, business, and IT persons) and a BCP and DRP development service are indicated as most important since these involve the entire organization while a technical IT-related service plays a critical role for system development and maintenance.**

***Keywords*— healthcare, information security, service, security as a service, blueprint**

I. Introduction

The service-oriented perspective of business has emerged in many industries, even small- and medium-sized companies in the last few years. Service innovation must begin with the recognition that services are solutions to customer needs as opposed to the traditional business model [1]. This is also similar to healthcare services. Information security in healthcare services is considered as an important concern since its personal information is very sensitive regarding privacy issues and health information system is related to human safety. However, information security in healthcare seems to be overlooked because of several reasons mainly related to lack of budget and lack of security awareness. Moreover, management does not have true understanding of how security relates to business objectives, in other words, the business processes cannot provide a proper balance between protection (security) and functionality (business productivity). As a result, truly service-oriented innovation and business blueprint cannot emerge.

Recent research shows that security in decentralized collaborative environments such as e-health challenges anyone from autonomous domains to access and share resources. Therefore, the need to create security awareness is very essential. The majority of the studies of healthcare IT security have been widely undertaken to highlight several success case studies in developed countries (such as the large number of cases of National Health Service-NHS of United Kingdom) or large-sized hospitals, whilst very few studies have been done in the context of developing countries or small-sized hospitals where show a number of distinctive characteristics such as (a) limitation of medical officer, IT person, IT infrastructure, IT skill, IT vision, and budget and (b) flat organizational structure. Despite this, high security level is still required, similar to large-sized hospitals.

The objective of this paper is to make a major contribution to a grounded understanding of development of information security as a service and a security blueprint for small-sized hospitals. The study conducts a survey using interview and observation techniques. Data were collected from medical officer and IT person, mostly the same person, and researchers themselves as participants. Following this section, the papers presents existing works related to this study. Then, the proposed a guideline for development of information security as a service and a security blueprint is presented and discussed. Finally, the conclusion is drawn.

II. Related Works

The protection of information, namely information security has been increasingly interested not only to increase organizations competiveness, but also to avoid criminals [2]. The primary goal of information security is *"to protect information and ensure that the availability, confidentiality and integrity of information are not compromised in any way"* [3]. Information security management is essential, focusing on the management of security risk, threats, and vulnerabilities, and it is suggested to be operated on a daily basis rather than an ad-hoc manner [3]. This becomes a trend in specialized areas like healthcare that concern this issue [4].

An organization should focus on information security awareness of the security environment and how this changes over time [5]. As reported in Kruger and Kearney [6], one of the objectives of security is *"to ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to*

reduce the risk of human error" [7]. Enforcing security awareness through education and training is hence paramount to meet this objective [2].

The concept of information security may be viewed from two issues: (a) technical information security issues, and (b) non-technical information security issues [3]. The technical information security issues emphasize knowing and understanding the adoption of IT to secure and protect information from unauthorized access [3, 8]. Generally, technical departments and employees with IT security skills are involved in IT security operation such as firewalls, encryption techniques, password protection, etc. [3]

In the field of healthcare systems, information security is considered as an important concern [9] since its personal information is very sensitive regarding privacy issue [10]. "Digital" patient's records need to be protected against unauthorized access [11].

Anderson [12] suggests that the level of security of electronic patient records must be similar to or higher than the standard used for paper records, yet patient confidentiality may be disclosed publicly. Recent research [4] shows that security in decentralized collaborative environments such as e-health challenges anyone from autonomous domains to access and share resources. In fact, not only privacy is concerned [13], other issues such as error issues, legal, business, and patient satisfaction are also important. Therefore, the need to create true understanding of information security in all aspects is very essential.

Understanding information security threats and challenges is important to avoid potential loss of information and knowledge assets [2]. While recent research on e-health mostly focuses on technical issues (for example,[10, 14, 15]), its research on soft issues especially focusing on awareness and user perception is very limited. Moreover, the majority of the studies have been widely undertaken to highlight several case studies in developed countries (such as the large number of cases of National Health Service-NHS of United Kingdom), whilst very few studies have been done in the cultural context of developing countries where the socio-cultural factors combined with the lack of resources and knowledge may present barriers to promote information security awareness [2].

Despite the emergence of service innovation in many industries, the service-oriented perspective of security in healthcare is very little mentioned in existing literature. A study of healthcare systems in Canada reveals that efficient and timely access to healthcare services is one of the key factors that lead to a profound impact on the well-being of individuals [16]. A method of "Security as a Service" (SeAAS) is proposed to develop architectural security blueprint in order to satisfy the requirements of the infrastructure specification with a focus on flexibility and maintainability [17]. Existing IT blueprint in healthcare sectors has been implemented for information sharing purposes – data standardization and interoperability [18], but not yet for information security service. Security is widely indicated as technical issues, but in contrast, service is more likely to be business terms. Hence, the challenge is how to link them together to create a blueprint for security services. Like a business model, a blueprint can be implemented through three factors i.e. organizational structures, processes, and systems [19].

III. FINDINGS

An interview protocol and an observation technique were designed to collect data from the identified targets, small-sized health care sectors in different part of local areas in Thailand in over three years. Medical officer and IT person, mostly the same person were interviewed and researchers themselves as participants.

The results show that most medical officers have computer proficiency and could use resources on the Internet. In most small-sized hospitals, there is no recruitment of IT personnel. Medical offers are able to operate on IT routine tasks that do not require in-depth technical skills. Most software and applications are developed by other hi-tech, large-sized hospitals or purchased from software vendors. In terms of security perception, they have shown its readiness in the basic level such as anti-virus software installation in all clients, password protection, and even disaster recovery plan. However, more training on security awareness and techniques is still required for them to reinforce users' good behavior and improve their technical skills.

The hospitals are very small and some have less than 10 officers. They may feel that they do not need an own security policy, even IT policy. They may adopt some IT-related policies deployed from the center (municipal hospitals or the Ministry of Public Health). Because of its small size, the organizational structures seem flat, as opposed to large-sized hospitals. Thus, it is easy to make sure that everyone can read the policy and the enforcement is not the problem.

As mentioned, they understand the need for basic access control to protect against unauthorized persons. In some hospitals, physical space in building is very limited. There are a few PCs working as both clients and servers and storing critical and sensitive data like patient's records. The concern is that these PCs are located in public areas and the space may be shared with waiting room, examination room and doctor office, where patients and guests can easily access. Although some hospitals have a server room, it is not equipped with a key lock or any control for verification of user identification and the entry is not recorded.

Although most small hospitals are situated within rural areas, telecommunication infrastructure is ready enough. Some use dial-up or ADSL modem to connect to the Internet or online applications. They must connect to the Virtual Private Network (VPN) provided through a third-party application when they want to transfer critical and sensitive data among hospitals.

The observation was also conducted during a disaster (2011 Thailand flood crisis). The first floor of many local hospitals was under water for a few months. IT infrastructures were moved to the upper floor. Temporary offices were established and shared with existing offices on the upper floor. Therefore, physical access control was loosened. For example, sensitive areas (computer rooms or data center) were not separated from public areas (waiting room) where patients or guests could easily access. However, in this situation, medical officers perceive that this practice is acceptable. It is observed that no critical IT infrastructures were damaged during the disaster. Most hospitals could continue their business during and after the disaster. This is because of the small size of hospital and small number of IT infrastructures. Also, they had an emergency plan and there was a good collaboration among local communities and authorities who could provide a great aid.

Security tends to be not concerned in terms of software development. As mentioned earlier, most applications in small hospitals are purchased from vendors or given by the center. Therefore, medical officers or IT persons do not know vulnerabilities that lead to security threats or risks in the application. Vendors or application developers may be hired for security maintenance such as updating patch. In most computers, anti-virus software is installed, but it is not updated on regular basis. Medical officers may feel that frequent update is time consuming. Also, they do not have enough time to learn the new version of application.

In terms of legal issues, most of small hospitals do not have security policies. In fact, some may have a general IT code of practice or term of use, but it is not compliant. Moreover, their security practices may be based on their own understanding. It is observed that at the present all public sectors including healthcare sectors are forced to develop their own information security policy and code of practice that are compliant with the national law. Small hospitals may adopt the policy and code of practice from the center such as municipality hospitals or the Ministry of Public Health.

IV. Security as a Service and Security Blueprint

This section aims to present factors linked to the results and findings from the survey. Then, it will provide a framework derived from the data, serving as a guideline for developing security as a service that leads to security blueprint for healthcare sectors.

Factors are presented in two dimensions. The first dimension, "security factors" is based on Certified Information Systems Security Professional (CISSP) domains drawn from various information security topics within the (ISC)²'s Common Body of Knowledge (CBK) [20]. The (ISC)² CBK is *"a taxonomy of topics relevant to information security professionals around the world, and establishes a common framework of information security terms and principles which allows information security professionals worldwide to discuss, debate, and resolve matters pertaining to the profession with a common understanding"* [20]. The domains include access control, telecommunications and network security, information security governance and risk management, software development security, cryptography, security architecture and design, operations security, business continuity and disaster recovery planning, legal and compliance, and physical and environmental security [21].

The second dimension, "business factors" is three business model factors for implementing a business blueprint including organizational structures, processes, and systems [19].

Table I below, presents these factors from two dimensions linked to the results and findings from the study. Access control is indicated as essential because it is a common solution to protect assets in organizations. Also, the factor like Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) is important. Since the hospital business deals with human safety, the hospitals must operate 24x7 and the systems need high availability. Therefore, the BCP and DRP factor should involve all people, processes and systems. However, cryptography is unlikely to be concerned. Cryptography has been embedded in most popular systems e.g. VPN and Database Management System (DBMS), thus, medical officers and IT persons in small hospitals may not need to learn.

Using the concept of business model and blueprint, the study can generate a security service blueprint. A summary of themes including a variety of services to be provided derived from the results above (Table I) is presented in the category of organizational structures, processes, and systems in Table II. Consulting service plays an important role in all three business factors because the consultant could help direct management persons, business persons, and IT persons in the proper methods of how to improve security and promote business at the same time. BCP and DRP development service is also involved in all aspects as confirmed in Table I. Legal service could survive an organization when security in a hospital is breached and customers (or patients) are affected by the security compromise. In the processes factor, a variety of services such as business service, auditing and assessment service, training service, and policy development service could help speed up in all processes and reduce learning curve. In systems factors, technical IT-related services are incorporated on an ease-of-use basis to ensure that users do not need to learn new technology: how to develop, use, install, upgrade, fix, and maintain. Moreover, most technical IT-related services are available on a pay-as-you-go basis that users only pay what they need.

TABLE I
RESULTS AND FINDINGS IN THE CATEGORY OF SECURITY FACTORS AND BUSINESS FACTORS

Factors	Organizational structures	Processes	Systems
Access control	• Access grant (e.g. role-based access control)	• Data classification	• Identification verification system • Authentication & authorization system
Telecommunication	N/A	• Dealing with service providers (e.g. contract, SLA)	• Network installation • VPN
Security governance & risk management	• Policy deployment • Management support	• Risk analysis • Training	N/A
Software development	N/A	• Dealing with software venders (e.g. contract, SLA)	• Anti-virus software
Cryptography	N/A	N/A	• Systems that encrypt data (e.g. VPN, DBMS)
Security architecture	• Choosing security model based on business model or organizational structures	N/A	N/A
Operations security	N/A	• Vulnerability test • Security audit • Backup & restoration	• Tools that support the processes
BCP & DRP	• Forming a BCP & DRP team or committee	• Plan implementation • Testing plan • Backup & restoration	• Channel to communicate during the disaster • Alternative site (off site)
Legal & compliance	• Assigning the responsible persons	• Developing policy	N/A
Physical security	N/A	• Entry and exit recording	• Systems that deny access to unauthorized person for sensitive areas

TABLE II
SECURITY SERVICE BLUEPRINT

Factors	Organizational structures	Processes	Systems
Services to be provided	• Consulting service (including management, business and IT) • BCP & DRP development service • Legal service	• Consulting service (including management, business and IT) • Business service • Risk and business impact analysis service • System Auditing and assessment service • Training service • Policy development service • BCP & DRP development service	• Consulting service (including management, business and IT) • System development service (software as a service) • Network service • IT maintenance service • BCP & DRP development service • Building service

V. CONCLUSIONS

The study has investigated the business and security factors that influence the development of security as a service and security blueprint. It demonstrates that the context of small-sized hospitals is unique from other hospitals, even other businesses in terms of information security. Small-sized hospitals have limitation of people, infrastructures and budgets whereas high level of security (confidentiality, integrity, and availability) is still required similar to other hospitals. Service-oriented approach is recommended to deal with this limitation to preserve security while business processes are not disrupted. Security blueprint could be implemented through three factors: organizational structures, processes, and systems. The proposed blueprint confirms that consulting service and BCP and DRP development service are indicated as most important as these are involved in the entire organization while technical IT-related service plays a critical role for system development and maintenance. A variety of services presented is provided on an ease-of-use and pay-as-

you-go basis where it helps improve processes and save budgets. Further investigation in other small-sized healthcare contexts is highly recommended to validate and test the blueprint, and then attempt to generalize it to the national level.

REFERENCES

[1] L. A. Bettencourt and S. W. Brown, "From goods to great: Service innovation in a product-dominant firm," *Business Horizons*, In Press, 2013.

[2] Y. Rezgui and A. Marks, "Information security awareness in higher education: An exploratory study," *Computers & Security*, vol. 27, pp. 241-253, 2008.

[3] E. Kritzinger and E. Smith, "Information security management: An information security retrieval and awareness model for industry," *Computers & Security*, vol. 27, pp. 224-231, 2008.

[4] O. Ajayi, R. Sinnott, and A. Stell, "Towards Decentralised Security Policies for e-Health Collaborations," in *Second International Conference on Emerging Security Information, Systems and Technologies, 2008*, Cap Esterel, France, 2008.

[5] A. B. Ruighaver, S. B. Maynard, and S. Chang, "Organisational security culture: Extending the end-user perspective," *Computers & Security*, vol. 26, pp. 56-62, 2007.

[6] H. A. Kruger and W. D. Kearney, "Consensus ranking – An ICT security awareness case study," *Computers & Security*, vol. 27, pp. 254-259, 2008.

[7] SANS 27001:2006, "South African National Standard. Information technology – security techniques – information security management systems – requirements," in *SANS 27001:2006, the identical implementation of ISO/IEC 27001:2005. 1st ed.* : Pretoria: Standards South Africa (a Division of SABS), 2006.

[8] E. Smith, E. Kritzinger, H. J. Oosthuizen, and S. H. Von Solms, "Information security education," in *the WISE 4 conference*, Moscow, Russia, 2004.

[9] E. Smith and J. H. P. Eloff, "Security in health-care information systems—current trends," *International Journal of Medical Informatics,*, vol. 54, pp. 39-54, 1999.

[10] M. Predeschly, P. Dadam, and H. Acker, "Security Challenges in Adaptive e-Health Processes," in *Computer Safety, Reliability, and Security*, M. D. Harrison and M.-A. Sujan, Eds. Berlin / Heidelberg: Springer, 2008.

[11] A. Appari and M. E. Johnson, "Information security and privacy in healthcare: current state of research," *International Journal of Internet and Enterprise Management* vol. 6, pp. 279-314, 2010.

[12] R. J. Anderson, "Security in Clinical Information Systems," *http://www.cl.cam.ac.uk/~rja14/policy11/policy11.html*, 1996.

[13] E.-H. W. Kluge, "Ethical and legal challenges for health telematics in a global world: Telehealth and the technological imperative," *International Journal of Medical Informatics*, vol. 80, pp. e1-e5, 2011.

[14] F. Ichihashi, Y. Sankai, and S. Kuno, "Development of Secure Data Management Server for "e-Health Promotion System"," *International Journal of Sport and Health Science*, vol. 4, pp. 617-627, 2006.

[15] S. Adibi and G. B. Agnew, "On The Diversity of eHealth Security Systems and Mechanisms," in *30th Annual International IEEE EMBS Conference*, Vancouver, Canada, 2008.

[16] G. Bhandari and A. Snowdon, "Design of a patient-centric, service-oriented health care navigation system for a local health integration network," *Behaviour & Information Technology*, vol. 31, pp. 275-285, 2012.

[17] B. Katt, T. Trojer, R. Breu, T. Schabetsberger, and F. Wozak, "Meeting EHR Security Requirement: SeAAS Approach," in *Seamless Care - Safe Care*, B. Blobel, Ed.: IOS Press, 2010.

[18] A. Kawtrakul, B. Kijsanayotin, and I. Mulasastra, "The Strategic Implementation of Data Interoperability for Better Health Care Services in Thailand," in *European Conference on e-Government*, Barcelona, Spain, 2012.

[19] A. Osterwalder and Y. Pigneur, *Business Model Generation*. Hoboken, New Jersey, USA: John Wiley, 2010.

[20] (ISC)², "About the (ISC)² CBK®," *https://www.isc2.org/cbk/Default.aspx*

[21] (ISC)², "CISSP® - Certified Information Systems Security Professional," *https://www.isc2.org/CISSP/Default.aspx*