International Journal of Innovative
Computing, Information and Control
Volume **8**, Number **11**, November **2012**

 ISSN 1349-4198
pp. **7865–7873**

AN EVALUATION MODEL OF INFORMATION SECURITY MANAGEMENT OF MEDICAL STAFF

Kuo-Hsiung Liao and Hao-En Chueh

Department of Information Management
Yuanpei University
No. 306, Yuanpei Street, Hsinchu 30015, Taiwan
{ liao; hechueh }@mail.ypu.edu.tw

Received July 2011; revised December 2011

Abstract. *With the advent of the computer age, well-organized information security management is vital for ensuring the sustainable growth of businesses or organizations. However, information security within an organization involves a number of levels, and most importantly, the "human" factor. Previous studies have not emphasized information security management issues. Medical organizations particularly have always neglected information security management issues. Information security issues can severely affect the quality of medical care, as well as the reputation and sustainable development of medical organizations. Thus, the primary purpose of this study is to assess the level of attention provided to information security management by medical personnel in Taiwan. This study developed an evaluation framework based on the ISO27001 standard for information security management, and surveyed personnel from two medical organizations in Taiwan. Risk priority numbers (RPNs) were used to assess the level of attention provided to information security management by medical personnel in Taiwan. The results indicate that information technology (IT) personnel pay great attention to information security management, whereas most executives have no technological knowledge. General staff have minimal technological knowledge and do not pay much attention to information security. These results mean that information security management cannot be fully implemented.*

Keywords: Information security management, Medical staff, Risk priority number (RPN), ISO27001

1. **Introduction.** Medical organizations in Taiwan face unprecedented challenges and impact to operations because of recent changes in the social environment, the implementation of National Health Insurance (NHI), and fierce competition within the industry. In response to these challenges, medical organizations have introduced IT solutions to enhance operational performance and increase the organization's competitive advantage. Recently, computer viruses and extensive hacking have caused severe information security disasters to every type of business in the world; medical organizations are no exception. The primary duty of medical organizations is to provide patients with excellent and appropriate care. When information system is not operated properly, the quality of medical care declines and the operational costs increase simultaneously. Therefore, establishing effective information security protection has become an extremely relevant issue [6]. Medical organizations particularly have always neglected information security management issues. Information security issues can severely affect the quality of medical care, as well as the reputation and sustainable development of medical organizations. Thus, the primary purpose of this study is to assess the level of attention provided to information security management by medical personnel in Taiwan.

Information security within an organization involves a number of levels, and most importantly, the "human" factor. Previous studies have not emphasized information security management issues. The information security generally required by medical organizations can be classified into two categories: products and management services. Products include firewalls, antivirus software, hacking detection [21], virtual private networks (VPN), and public key infrastructure (PKI), whereas management services comprise assistance in establishing information security policies, integrating existing systems, acquiring information security certification [14], and outsourcing the management of information security systems.

Strengthening information security is crucial to enable consumers to purchase goods online securely. Additionally, medical personnel have limited knowledge of information security measures, such as encryption and decryption technology, firewalls, hacker prevention, or virus protection [22]. Although today's market still focuses more on products, the conceptual shift in information security protection has increased public emphasis on the management of security services. Most systems do not consider patients' rights or how to identify the information sender [1]. Information security within an organization comprises numerous levels; previous studies have frequently neglected the most important aspect, the human factor. Therefore, we propose that a well-planned information security management system and greater emphasis on information security management among medical personnel can ameliorate the various security issues currently faced in medical organizations.

Information security systems in most medical organizations employ the ISO27001 standard for managing information security. This standard comprises 11 key points of control, 39 objective controls, and 133 control items. With such an abundance of objective controls and control items, most medical personnel struggle to understand the connotations and significance thoroughly. This has led to negligence of specific objective controls and control items, and created vulnerabilities in the security management of medical organizations.

The primary purpose of this study is to evaluate the level of attention that medical personnel give to information security management in medical organizations in Taiwan. This study developed an evaluation framework based on the ISO27001 standard for information security management and interviewed medical personnel from two medical organizations in Taiwan. RPN was used to assess the value medical personnel place on information security management. The results indicate that information technology (IT) personnel pay great attention to information security management, whereas most executives have no technological knowledge. General staff have minimal technological knowledge and do not pay much attention to information security. These results mean that information security management cannot be fully implemented. The results may benefit medical organizations by increasing awareness and knowledge of information security management and enhance the establishment of an effective information security protection environment.

2. **Information Security for Organizations.**

Scholars have proposed various definitions of "information security." With the advent of the digital age, the definition of information security has gradually shifted from a technological product perspective to a management perspective. This indicates that information security is a management issue rather than a technological issue.

In a conference in 2001, the Organization for Economic Co-operation and Development [18] defined the goal of information security as "protecting the interests of those relying on information systems from harm resulting from failures of availability, confidentiality, and integrity."

TABLE 1. Definition of information security

Source	*Definition*
IBM (1984) [11]	*Protection of information assets from either deliberate or accidental unauthorized disclosure, modification, destruction, or invalidation.*
L. Huang (1992) [10]	*Applying management procedures and security protection technologies on computer software and data to ensure that data in storage or transmission are protected from being either deliberately or accidental accessed, deleted, or modified by a third party.*
K. Liu (1995) [17]	*The protection scope for computer security involves tangible and intangible elements, including the control room, host computer, terminal, network cable, software, and data. Sound security measures maintain the confidentiality, authenticity or integrity, and availability of data.*
Arthur et al. (1995) [2]	*Information security threats can be classified as potential threats, physical disasters, technical failures, human errors, data abuse, and data loss.*
Parker (1997) [19]	*Information security is the protection of the oral, printed, and automatically recorded information of an individual or organization, as well as protection of the generation, processing, transmission, storage use, display, and control of information.*
T. Finne (2000) [9]	*Various measures adopted for reducing information risks.*

Confidentiality: to ensure only authorized individuals can access information.

Authenticity or integrity: accuracy and integrity of the information protection and processing technology.

Availability: to ensure the authorized individuals can obtain information and related assets whenever required.

The confidentiality, authenticity, and availability of information are underlying elements that ensure the competitiveness, smooth cash deployment, and profitability of an organization conforming to legal standards and possessing a good business image. However, the authenticity and availability of information often appear more important to numerous organizations, leading to an unbalanced situation because of management negligence. Organizations aim to achieve ensure confidentiality and data protection; however, this frequently leads to the inconvenience of data access. This is how hackers steal data and why organizations most update their data security protection measures continually.

The ISO27001 [12] is an extensive information security management standard employed by businesses and organizations; it provides the most comprehensive reference specification for information security management in the world. In other words, the ISO27001 framework establishes standards for the information security management systems in organizations based on risk and crisis management.

According to OECD, the advent of the information technology age has not only accelerated the growth of individual knowledge and industry applications, but has also boosted globalization. Requirements for information security have also continuously increased. Thus, the OECD Committee for Information, Computer, and Communications Policy proposed a guideline for information security systems in 1990; this guideline was officially approved in 1992.

In 1993, Britain's Department of Trade and Industry (DTI) published an information security management standard. Subsequently, the British Standards Institution (BSI) proposed the BS7799 Part I Code of Practice for Information Security Management in February 1995. In 1998, the BS7799 Part II Information Security Management Systems – Specification with Guidance for Use was published. An amendment to BS7799 Parts I and II was published in May 1999.

Upon its approval in November 2000, the BS7799 Part I became the information security system standard known as ISO17799:2000, which was commonly adopted by organizations worldwide. In 2005, this standard was amended and republished as ISO17799:2005; the BS7799 Part II was published as ISO27001:2005. The main difference between the ISO17799:2005 and ISO27001 is that ISO17799 acts as a guide for information security imports, whereas ISO27001 is an integrated information security verification standard. Businesses or organizations can establish an information security management system that matches their needs using the ISO27001 mechanisms.

In practical applications to establish internal information security management systems, ISO27001 has 11 key points of control that comprise 39 objective controls and 133 control items.

For medical organizations, the advantages of establishing security management can be divided into internal and external advantages. Internally, establishing security management can improve the information security environment of a medical organization, reduce risk during information transactions, and enhance organizational profitability. Externally, establishing security management enhances patients' confidence and satisfaction with the medical organization and strengthens the organization's market competitiveness. Although ISO27001 is not the only standard for establishing security management systems, it has the most integrated explanations for constructing a complete information security framework; thus, it has become the most commonly adopted mainstream information security standard.

3. **Research Method.** Although more medical organizations are implementing information security practices than before, the wide range of key control points, objective controls, and control items in ISO27001 present a substantial challenge for medical personnel. To understand the degree of emphasis and knowledge of information security management issues among medical personnel, this study developed an evaluation framework based on ISO27001 and interviewed personnel from two medical organizations in Taiwan. RPN [5,15,20] was used to assess the degree of emphasis personnel given to information security management.

To conduct qualitative risk analysis during project management, organizations are often expected to focus on high-priority risks and establish a countermeasure strategy according to enhanced project performance. Additionally, more organizational resources are allocated to preventing, detecting, and responding to risk. To define high-priority risk, we typically score the recognized risks listed in the risk list based on level of impact. Then we multiply this score with the probability of occurrence. The combination of the probability and impact represent the "risk index." Finally, we contrast the probability with the impact matrix to determine whether the risk is high, medium, or low. Risk indices calculated by multiplying the impact with probability are commonly seen in numerous books on problem analysis and decision making. In the decision making process, evaluating the risks of available project options to eliminate projects with higher risk is a commonly used method. In addition, manufacturers have also widely employed the failure mode and effect analysis. For this, the RPN follows an identical concept and is calculated according to severity (S), occurrence (O), and detection (D), RPN = O * S * D. This

allows managers to focus on risks with a high severity and high occurrence rating, and those that are difficult to detect in advance.

To evaluate the occurrence, severity, and detection when calculating the RPN, the three indices are divided into five levels each. Next, the three indices are multiplied and the resulting value is the RPN. The three indices and varying levels are described below.

Occurrence: the occurrence frequency of the considered aspects is used to determine the level, as shown in Table 2.

Table 2. Occurrence

Value	*Severity Level*	*Occurrence frequency*
1	*Very low*	*Once per year (or more than once per year)*
2	*Low*	*Once per quarter (or more than once per quarter)*
3	*Medium*	*Once per month (or more than once per month)*
4	*High*	*Once per week (or more than once per week)*
5	*Very High*	*Continuous/daily occurrence*

Severity: information security in hospitals can impact the environment differently according to various information security qualities. Greater organizational output tends to increase a hospital's information security and resource consumption. Severity can be divided into various levels, as shown in Table 3.

Table 3. Severity

Value	*Severity Level*	*Emergency/Abnormal Situation*
1	*Very low*	*The situation can be resolved immediately*
2	*Low*	*The situation can be resolved immediately, but it could lead to possible losses*
3	*Medium*	*The situation requires external assistance and could lead to slight losses*
4	*High*	*The situation requires external assistance and will lead to severe losses*
5	*Very High*	*The situation cannot be resolved and will lead to severe losses*

Detectivity: the degree of abnormality or impact on a hospital's information security that can be detected by the organization's staff or patients, as shown in Table 4.

For general applications of the FMEA method, improvements should be prioritized according to their RPN score. A higher RPN score denotes a greater priority for improvement.

4. **Case Study.** The purpose of this study is to evaluate the degree of emphasis and knowledge of information security among personnel from medical organizations in Taiwan. For this study, we selected personnel from two regional medical organizations and conducted a questionnaire survey. Basic information of the two regional medical organizations is shown in Table 5.

This study used the following experimental procedures.

The questionnaire was developed according to the control items in ISO27001, and distributed among personnel from two regional medical organizations.

A total of 10 questionnaires were distributed in two regional medical organizations. We collected 5 questionnaires from Hospital A, but only 3 questionnaires from Hospital

Table 4. Detection

Value	*Severity Level*	*Degree of abnormality or impact on a hospital's information security that can be detected by the hospital or patients*
1	*Very low*	*Abnormality or impact can be discovered by visual inspection or sensory perception*
2	*Low*	*Abnormality or impact can be discovered by software or hardware*
3	*Medium*	*The hospital has not purchased relevant software or hardware for immediate detection*
4	*High*	*No relevant detection software or hardware is currently on the market*
5	*Very High*	*Cannot be detected or examined*

Table 5. Basic information of hospitals

Item	*Hospital A*	*Hospital B*
Number of medical personnel	*400*	*700*
Total units of computer equipment	*500*	*400*
Contains an independent information technology (IT) department	*Yes*	*Yes*
Number of IT personnel	*3*	*7*

B. Only 3 of the questionnaires from Hospital A were valid for this study, whereas all 3 questionnaires from Hospital B were valid.

We then calculated the RPN for each control item in the questionnaire.

Subsequently, we compiled the collected data and conduct an analysis and comparison according to the suggestions of experts.

After evaluating the degree of emphasis and knowledge regarding information security of personnel from two regional medical organizations, we further analyzed the evaluation results using actual data obtained through expert observation and verification. The results revealed a correlation between the degree of emphasis and information security knowledge and the actual performance of personnel from two regional medical organizations.

5. **Discussion.** After summarizing the RPN values, we have derived the following conclusions. Hospital A had a more thorough security policy. In Hospital B, only IT personnel emphasized security policies. Additionally, general staff had no clear communication with senior executives regarding security policies, and did implement or follow these security policies. The senior executives and IT personnel in Hospital A emphasized organizational security; whereas, in Hospital B, only IT personnel emphasized organizational security issues.

In both hospitals, only IT personnel emphasized asset classification and control. This may be because other staff has no knowledge of asset classification and control.

Only general staff from Hospital B had low results. This indicates that the general staff from Hospital B do not emphasize communications, operations management, and access control.

Significant differences between the results of the two hospitals were found. From the evenly distributed data, Hospital A showed a more favorable performance. The senior executives of Hospital B also scored poorly, possibly because the general staff had no

Table 6. RPN values

Item	*Hospital A*			*Hospital B*		
	Senior Manager	*IT Staff*	*Operator*	*Senior Manager*	*IT Staff*	*Operator*
Information security policy	*84*	*84*	*84*	*56*	*84*	*28*
Organization of information security	*306*	*306*	*251*	*241*	*403*	*129*
Asset management	*102*	*118*	*102*	*109*	*143*	*116*
Human resource security	*360*	*360*	*335*	*324*	*472*	*260*
Physical and environmental security	*545*	*552*	*352*	*557*	*656*	*539*
Communications and operations management	*1068*	*1068*	*902*	*1117*	*1327*	*687*
Access control	*1299*	*1340*	*1125*	*1635*	*1698*	*1137*
Information systems acquisition, development, and maintenance	*732*	*688*	*704*	*844*	*840*	*536*
Information security incident management	*360*	*360*	*335*	*260*	*472*	*324*
Business continuity management	*198*	*198*	*198*	*198*	*246*	*164*
Compliance	*397*	*397*	*349*	*442*	*399*	*292*
SUM	*5367*	*5387*	*4653*	*5827*	*6470*	*4148*

understanding of the development and maintenance of information security systems. Although both hospitals IT personnel placed the greatest emphasis on information security management and had the most knowledge, an inverse result was found in the other two hospital staff groups. Regarding personnel security, Hospital B performed better than Hospital A did.

In both hospitals, only IT personnel emphasized the risk management of information security. Most senior executives had minimal knowledge of this technology, and general staff showed minimal knowledge and did not place much emphasis on information security. Thus, these hospitals primarily require a bottom-up reporting policy and top-down implementation.

6. **Conclusion.** To improve information security management performance in medical organizations, we propose the following recommendations according to study results.

Security policy: organizations should primarily emphasize projects developed by the information management office and enhance the awareness and training of general staff.

Organizational security: information security policies should be promoted in a top-down manner to meet inspection requirements. Strategies addressing vulnerabilities in post-disaster recovery, remote backup services, server patching, or other matters related to information security have been developed, but should be implemented more thoroughly.

Asset classification and control: asset classification and the corresponding safeguard measures were considered insufficient. The users were unable to implement these measures when the standard operation procedures were in place. No hierarchical difference existed between the groups; thus, we could not limit group members because of substantial complicity. We recommend that the information management office develop measures for improvement.

Personnel security: corresponding agreements (on confidentiality and intellectual property rights) regarding third-party access are currently in place. However, an actual education or training program for staff is not provided. There is an information security management system that monitors accidents, fault types, quantity, and cost of lost time. Quantified data are stored in the main computer system rather than on personal computers; however, data backups are copied from personal computers. No written operational procedures regarding file backups exist; this is conducted only upon verbal request. Penalties for security breaches are only reflected in the employee's evaluation. However, communicating with staff that is not following instructions regarding the occurrence of incidents is important. We recommend adjusting training requirements to include clarifying the information security responsibilities of personnel.

REFERENCES

[1] H. O. Alanazi, H. A. Jalab, G. M. Alam, B. B. Zaidan and A. A. Zaidan, Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance, *Journal of Medicinal Plants Research*, vol.4, no.19, pp.2059-2074, 2010.

[2] E. Arthur, S. Bosworth and D. Hoyt, *Computer Security Handbook*, Native Intelligence, Inc., 1995

[3] British Standards Institution, Information security management – Part 1: Code of practice for information security management, *BS 7799-1*, 1999.

[4] British Standards Institution, Information security management – Part 2: Specification for information security management systems, *BS 7799-2*, 1999.

[5] L. Chao, *Application of FMEA at the Early Stage of TPM*, Master Thesis, Chaoyang University of Technology, 2002.

[6] C.-H. Chen, A security mechanism for protecting the customer privacy when purchasing digital products, *ICIC Express Letters, Part B: Applications*, vol.2, no.2, pp.487-492, 2011.

[7] R. Chen, C. Liu and J. Hsiao, The BS7799-based framework for building integrated information security research hospital, *Proc. of the International Medical News Conference*, Chiayi, Taiwan, pp.100-105, 2004.

[8] K. Farn, Introduction of the purpose and application of information control and related technology, *Information Security Newsletter*, vol.8, pp.1-7, 1999.

[9] T. Finne, Information systems risk management: Key concepts and business processes, *Computers & Security*, vol.19, pp.234-247, 2000.

[10] L. Y. Huang, *Information Security Planning and Management*, SongKang Books, Taipei, 1992.

[11] IBM, *IBM Data Security Support Programs*, USA, 1984.

[12] ISO International Standards for Business, Government and Society, Information security management systems – Requirements, *ISO 27001*, 2005

[13] S. Li, *Information Security*, Wenkui Books, Taipei, 2007.

[14] Y.-L. Lin and C.-L. Hsu, Cryptanalysis and improvement of a hierarchical key management scheme for access control in the mobile agent, *ICIC Express Letters*, vol.4, no.1, pp.183-187, 2010.

[15] C. Liu, *Integrating Failure Mode and Effect Analysis with Economic Quality Cost Model for Healthcare Industry*, Master Thesis, National Cheng Kung University, 2009.

[16] D. Liu, From risk management to create information security fortress, *Communication Magazine*, pp.94-99, 2001.

[17] K. Liu, *Information Security*, Scholars Books, Taipei, 1995.

[18] Organization for Economic Cooperation and Development, Information Security Objective, *OECD Guidelines for the Security of Information Systems*, 2001.

[19] D. Parker, Information security in a nutshell, *Information Systems Security*, pp.16-25, 1997.

[20] Y. Wang, *Identifying Significant Environmental Aspect by FMEA: A Case Study*, Master Thesis, Feng Chia University, 2004.

[21] S. Wu, J. Yu, X. Fan and X. Tang, An effective attack classification scheme for intrusion detection systems using Bayesian analysis techniques, *ICIC Express Letters, Part B: Applications*, vol.2, no.6, pp.1253-1259, 2011.

[22] C. Yao and C. Jong, Perceived risk of information security and privacy in online shopping: A study of environmentally sustainable products, *African Journal of Business Management*, vol.4, no.18, pp.4057-4066, 2010.