Medical Organization Information Security Management Based on ISO27001 Information Security Standard

Kuo-Hsiung Liao and Hao-En Chueh
Information Management Department, Yuanpei University, HsinChu, Taiwan.
Email: {liao, hechueh}@mail.ypu.edu.tw

***Abstract*—Most of the information security events in medical organizations are due to improper management. This is a clear indication that the security of information is an issue related to information and communication technology and a management issue as well. In a review of literature, most research on information security has focused on information and communication technology issues, such as network security and access control; rarely addressing issues at the management-level. The main purpose of this study is to construct a mechanism for the management of information with regard to security as it applies to medical organizations. This mechanism is based on the eleven control items and one hundred thirty-three control objectives of the ISO27001 information security management standard. This study analyzes and identifies the most common events related to information security in medical organizations and categorizes these events as high-risk, transferable-risk, and controlled-risk to facilitate the management of such risk.**

***Index Terms*—Medical organizations, Information security, ISO27001, Risk management, Access control**

I. Introduction

According to the Organization for Economic Cooperation and Development (ECD), the objective of information security is "to ensure the various interests which rely on the information system, avoid harm created by the loss of confidentiality, integrity, and availability" [5, 9, 14]. With recent outbreaks of computer viruses and hacker intrusion, numerous domestic and foreign enterprises have reported severe breaches in the security systems related to information, and both public and private medical organizations are no exception. Because the primary responsibility of medical organizations is to provide patients with quality care, information security events quickly leave a medical organization incapable of carrying out normal operations, with negative consequences for the rights of patients. Therefore, the means to build an information security management mechanism to protect medical organizations has become an issue of crucial importance.

Past research on information security has constantly stressed the need for information and communication technology (ICT) such as data encryption, firewall technology, and computer viruses. However, the importance of maintaining the security of medical organizations lies not only in protecting important information from theft, forgery, or damage; more importantly, information security safeguards the reputation, value, and sustainable development of the medical organization. For this reason, information security is an issue of information and communication technology as well as an issue at the management-level. To avoid repeated information security events, it is essential to establish a mechanism for the effective management of information security.

To help enterprises achieve information security goals, the British Standards Institution (BSI) has published the BS7799 information security management standard in 1995, and then became ISO 27001 international standard in 2005 [1, 14], covering all aspects of information security. Current literature on risk management can only provide people with applications of risk management to information security. These studies are unable to provide a clearly quantitative, indexed description or applicable methods for managing risk related to assets, personnel, or other threats and vulnerabilities created by various information security risks [18]. Therefore, the main purpose of this study was to implement the eleven control items and one hundred thirty-three control objectives of the ISO27001 information security management standard as a foundation for the protection of information and establish a mechanism for the management of information security applicable to medical organizations. In this paper, we analyze and identify the most common information security events for medical organizations and categorize these events as high-risk, transferable-risk, and controlled-risk for the benefit of managing risk with regard to the information of medical organizations.

II. Literature Review

The frequency of information security events in medical organizations has been attracting increased attention to medical organization security issues. According to Smith and Eloff [15], the scope of security protection for medical organizations should include assistance in avoiding:

(1) physical damage to persons or property;
(2) privacy violations;

doi:10.4304/jsw.7.4.792-797

(3) loss or destruction of medical information;
(4) harm to operational integrity or consistency.

In designing security systems for medical organizations, Smith and Eloff proposed that the first step be the careful identification and analysis of the existing threats to personnel, assets, and information, and assessing resilience to such vulnerabilities. Secondly, assessing potential threats helps to establish security countermeasures. Therefore, programming information security for medical organizations must be considered from the perspective of a comprehensive security protection , including: defining the scope of system security protection, assessing risks, establishing internal control and auditing systems, exploring other management-related issues, and structuring the comprehensive needs for information security of medical organizations.

The characteristics of harmful information security events usually include behavioral uncertainty, unpredictability, and the inability to understand what true security is. In one way, risk management improves the performance and the effectiveness of evaluation with regard to information security. After enhancing awareness of information security, organizations can use resources more efficiently, create better project management, and minimize waste. Willett (1901) [23] believed that "risk" and "chance" were different and that they should be distinguished by using "the degree of probability" for chance and "the degree of uncertainty" for risk. But generally speaking, risk can be defined in two ways [1]: first, the uncertainty of an accident; second, the chance of loss caused by the accident. Song (1993) [19] defined that risk based on three factors: first, on security needs; second, on risk-created costs; and third, on the requirements of government regulations. The general steps in managing risk are: first, identifying the risk; second, measuring the risk; third, selecting the proper tools; fourth, taking action; fifth, evaluating the performance.

Because a single information security event could trigger a chain of issues, dealing with information security events arbitrarily may cause unforeseen error and losses Therefore, security management practices have been established in several advanced countries to assist enterprises and office personnel in managing systems and operating data.

The United States has information security operating standards such as Control Objectives for Information and Related Technology (COBIT), Trusted Computer System Evaluation Criteria (TCSEC), while the United Kingdom has introduced the ISO27001 information security management standard. Control Objectives for Information and Related Technology, the operating standard published by Information Systems Audit and Control Association (ISACA) in 1995, is a set of comprehensive considerations based on information technology control standards and information technology as security. Trusted Computer System Evaluation Criteria, proposed by the U.S. National Computer Security Commission (NCSC) in 1983, takes a systematic approach by dividing security issues into four categories, named A, B, C, and D, where the category of computer systems dictates the standard level of security required. The aim of the ISO27001 information security management standard, developed by BSI, was to ensure the security of business information assets including software and hardware facilities as well as data and information, by avoiding information security-related damage caused by internal and external threats as well as operating mistakes of organizational staff. Simply put, the objective of ISO27001 was to establish a comprehensive information security management system by ensuring information confidentiality, integrity, and availability [1, 3, 5, 9, 14].

Due to the characteristics of each standard, the methods for dealing with and assessing information security differ. Each standard has its own suitable application, but from the perspective of information security management for medical organizations, ISO27001 is best suited to ensuring the security of medical organizations and their information-related assets. The ISO27001 information security management standard has eleven control items and one hundred trirty-three control objectives, including the protection of software and hardware facilities, information, and avoiding various internal and external threats as well as operating mistakes of organizational staff. It also covers various aspects of security policy, from formulating policy related to security and delegating security related responsibilities to assessing risk and access control. In short, ISO27001 could be described as a comprehensive information security management standard. As for studies applying ISO27001 to the medical industry, Janczewski (2002) [15] researched the use of ISO27001 to develop the Healthcare Information System (HIS), and investigated the basic security infrastructure behind the development of HIS, and made fundamental recommendations for security-related issues in the development of HIS.

In practical application in establishing internal information security management systems, ISO27001 has 11 key points of control that comprise 39 objective controls and 133 control items. The 11 key points are listed below:

(1) Security Policy: Define and document the expectations and requirements of middle and senior managers for information security, to facilitate information security within the organization.

(2) Organization of Information Security: Establish a specific information security department and define its organizational structure, operational processes, and responsibilities.

(3) Asset Management: Classify and value information according to its operational process and asset value within the organization, and plan safeguard measures for assets at different levels.

(4) Human Resources Security: Most information security issues originate from human error. Planning of

staff training, job description, responsibilities, and critical event reporting procedures should be carried out to reduce the probability of human error and willful infringement.

(5) Physical and Environmental Security: Standardize the safeguard measures, security equipment, and control framework for tangible assets, such as access control systems, surveillance cameras, and time lock.

(6) Communications and Operations Management: Communication and operation management refers to the control mechanism that ensures normal operation of IT facilities.

(7) Access Control: A user's data access rights should be set according to the user's job authority in order to decrease the risk of unauthorized access to system resources.

(8) Information System Acquisition, Development and Maintenance: Plan the system development and maintenance process to include information security in the scope of operational processes.

(9) Business Continuity Management: Plan emergency measures and recovery mechanisms for critical information security events of an organization.

(10) Compliance: Protect the organization from violating laws and regulations corresponding to information security management systems, and examine and improve the control processes in accordance with the current legal environment.

(11) Information Security Incident Management: Evaluate information recording methods for occurrence of information security events and discuss ways to avoid repeat occurrences of the event after issues are resolved.

For medical organizations, advantages of establishment of security management can be divided into internal and external advantages. Internally, establishment of security management can improve the information security environment of a medical organization, reduce risk in information transactions, and enhance organizational profitability. Externally, establishment of security management enhances patients' confidence and satisfaction in the medical organization, and strengthens the market competitiveness of the organizations. ISO27001 is not the only standard for security management system establishment. But it has the most integrated explanations on how to construct a complete information security framework, and so has become the most commonly adopted mainstream information security standard

III. Research Methods

Although the level of attention paid and practice made by many medical organizations regarding information security have increased, the means by which medical organizations value information assets, assess security threats, understand weaknesses in the organization, establish vigilance toward information security among its staff, and develop information security policy is an issue that must be considered to establish an effective mechanism for information security management. The main purpose of this study was to help medical organizations to use the most appropriate resources to build the most effective mechanism for information security management.

This study uses the eleven control items and one hundred thirty-three control objectives of the ISO27001 information security management standard as the foundation to establishing a mechanism for the information security management suitable for medical organizations. This study first identified all information assets, information security threats, and information security vulnerabilities within the organization based on ISO27001's one hundred thirty-three control objectives, and formed a risk assessment scale through the assessment of the probability of occurrence and the degree of impact posed by security events. Then, according to the assessments of experts, we set weightings, ranked the information security events in order of priority, and structured a security management model.

Carroll [1] proposed a mathematical formula for using annualized loss expectancy (ALE) to assess the necessary cost of asset protection and losses due to information threats. The formula is as follows:

$$ALE = TV \tag{1}$$

Here, T is the annual value of a given threat, while V is the estimated value of assets. To evaluate the value at risk (VaR) of ISO27001 control objectives, we convert the value T into the control objective's probability of occurrence (value P), and convert the value V into the control objective's degree of impact (value I). The ALE is then regarded as evaluating the VaR for each information security control objective.

$$PI = VaR \tag{2}$$

Using the 133 control objectives in ISO27001 as a framework, we build an assessment table for the information security management according to each objective's probability of occurrence (value P) and their degree of impact (value I).

The comparative tables of probability and impact are shown in Tables 1 and Tables 2, respectively.

TABLE 1.
THE COMPARATIVE TABLE FOR THE GIVEN METHOD OF VALUE P (PROBABILITY)

Probability	Comparative Value
0.00 ~ 0.20	1
0.21 ~ 0.40	2
0.41 ~ 0.60	3
0.61 ~ 0.80	4
0.81 ~ 1.00	5

TABLE 2.
THE COMPARATIVE TABLE FOR THE GIVEN METHOD OF VALUE I (IMPACT)

Degree of Impact	Comparative Value
No Impact	1
Slight Impact	2
Some Impact	3
Large Impact	4
Significant Impact	5

To more effectively evaluate information security risk and select the appropriate response, Halliday (1996) [13] again used the numerical values 1 to 5 for the probability of occurrence and the degree of impact to express respective risk quadrants, as shown in Table 3, Figure 1 and Figure 2.

TABLE 3.
THE COMPARATIVE TABLE FOR FREQUENCY AND IMPACT VALUE

Risk Quadrant	Value P (Probability)	Value I (Impact)
Q1	1 < P ≦3	1 < I ≦3
Q2	3 < P ≦5	3 < I ≦5
Q3	1 <P ≦3	3 < I ≦5
Q4	3 < P ≦5	1 < I ≦3

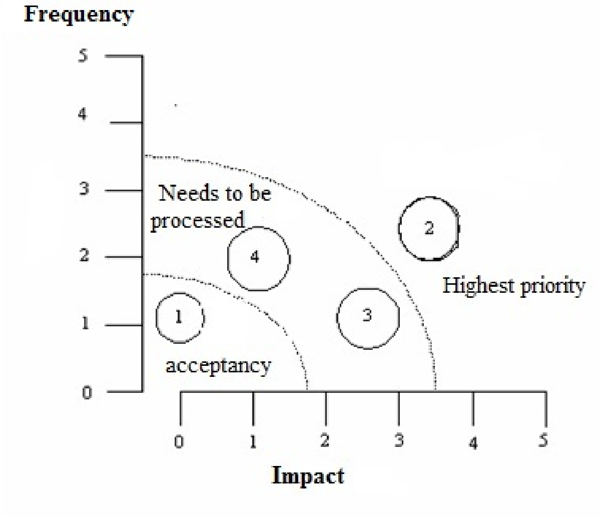

Figure 1. Risk Priority (Halliday, 1996) [13]

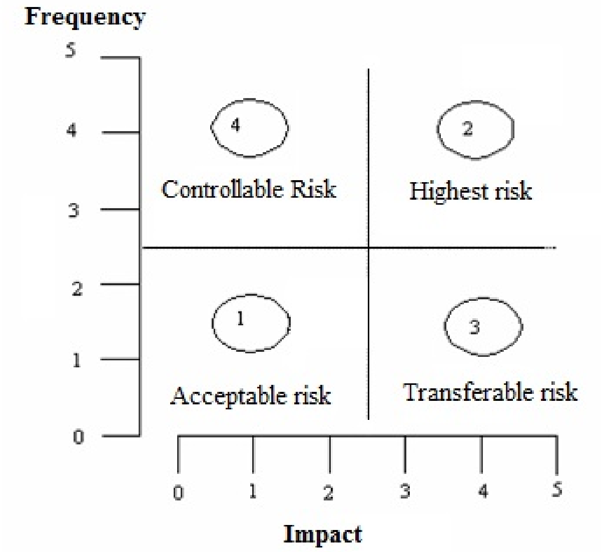

Figure 2. Risk Quadrants (Halliday, 1996) [13]
{Frequency; Impact; Q1: Acceptable Risk; Q2: High Risk (Decrease Risk & Decrease Frequency); Q3: Transferable Risk; Q4: Controllable Risk (Decrease Frequency)}

Information security management mechanisms constructed in this way are not always the best model. Therefore, they must be continually assessed to maintain effectiveness in risk management.

IV. EXPERIMENTS AND RESULTS

The main purpose of this study was to establish a risk assessment table for the control items of the ISO27001 information security management standard, and evaluate (through expert interviews), their probability of occurrence (value P) and degree of impact (value I). In this manner, we hoped to establish the VaR in the ISO27001 information security management assessment table. The steps taken are described below:

(1) Questionnaire Design: We produced a questionnaire based on the one hundred thirty-three control items of the ISO27001 information security management standard.

(2) Expert Recommendations: We invited six information security experts to provide relevant values for the probability of occurrence and degree of impact for the questionnaire, as shown in Table 5.

(3) Retrieval of Questionnaire and Data Analysis: We recovered the expert opinions and calculated the value at risk.

(4) Synthesis of Risk Assessment Data: We established a mechanism for the management of information security for medical organization according to the expert opinions.

This management mechanisms constructed in this study's can be seen in Table 4, Table 5 and Table 6.

TABLE 4.
HIGH RISK(Q2) OF INFORMATION SECURITY MANAGEMENT MECHANISMS

Control Item	Procedural Order
1-1 Information security policy document 2-3 Allocation of information security responsibilities 2-4 Authorization process for information processing facilities 3-1 Inventory of assets 4-10 Disciplinary process 5-1Physical security perimeter 5-2 Physical entry controls 5-3 Securing offices, rooms and facilities 5-8 Cabling security 5-9 Equipment maintenance 6-1 Documented operating procedures 6-2 Change management 6-8 System acceptance 6-9 Controls against malicious software 6-10 Information back-up 6-13 Network controls 6-14 Management of removable computer media 6-15 Media handling 6-17 Security of system documentation 7-2 User registration 7-4 User password management 7-6 Password use 7-7 Unattended user equipment 7-8 Policy on use of network services 7-9 Enforced path 7-11 Node authentication 7-13 Segregation in networks 7-14 Network connection control 7-15 Network routing control 7-17 Automatic terminal identification 7-19 User identification and authentication 7-20 Password management system 7-21 Use of system utilities 7-23 Terminal time-out 7-25 Information access restriction	Highest priority

7-26 Sensitive system isolation	
7-27 Event logging	
7-28 Monitoring system use	
8-1 Security requirements analysis and specification	
8-2 Input data validation	
8-10 Key management	
8-13Access control to program source library	
8-14 Change control procedures	
8-18 Outsourced software development	
9-1 Information security awareness, education and training	
9-2 Management responsibilities	
9-3 Incident management procedures	
10-1 Business continuity management process	
10-2 Business continuity and impact analysis	
10-3 Developing and implementing continuity plans	
11-2 Intellectual property rights	
11-3 Protection of organizational records	
11-4 Data protection and privacy of personnel information	
11-6 Regulation of cryptographic controls	

TABLE 5.
TRANSFERABLE RISK(Q3) OF INFORMATION SECURITY MANAGEMENT MECHANISMS

2-2 Information security co-ordination	Needs to be processed
2-6 Contact with authorities	
2-8 Independent review of information security	
5-6 Equipment sitting and protection	
5-12 Secure disposal or re-use of equipment	
5-13 Removal of property	
6-6 External facilities management	
6-12 Fault logging	
6-16 Information handling procedures	
6-20 Physical media in transit	
6-21 Electronic messaging	
6-22 Business information systems	
7-3 Privilege management	
7-10User authentication for external connections	
7-12 Remote diagnostic port protection	
7-16 Security of network services	
7-24 Limitation of connection time	
8-3 Control of internal processing	
8-4 Message integrity	
8-5 Output data validation	
8-6 Policy on use of cryptographic controls	
8-11 Control of operational software	
8-12 Protection of system test data	

TABLE 6.
CONTROLLED RISK (Q4) OF INFORMATION SECURITY MANAGEMENT MECHANISMS

1-2 Review of the information security policy	Needs to be processed
4-1 Roles and responsibilities	
4-8 Removal of access rights	
5-7 Working in secure areas	
6-5 Separation of development, test and operational facilities	
7-1 Access control policy	
7-5 Review of user access rights	
7-30 Mobile computing	
8-15 Technical review of operating system changes	
8-16 Restrictions on changes to software packages	
11-5 Prevention of misuse of information processing facilities	

V. CONCLUSION

A well-planned information security management system to medical personnel can ameliorate the various security issues currently confronting medical organizations. Given the competitive climate in the medical industry, with the expansion of hospitals, changes in government policy, and increasing demand for quality medical service, many hospitals have had to face unprecedented operational pressures, forcing hospital operators to pay closer attention to costs. The mechanisms for the information security management developed in this study could help medical organizations to assess their level of information security risk and identify appropriate improvement strategies. To improve information security management performance in medical organizations, the following recommendations are proposed. Security policy: mainly focus on projects developed by the information management office and enhancing promotion and training on general staff. Organizational security: information security policies should be promoted in a top-down manner to meet inspection requirements. The loop holes in post-disaster recovery, remote backup, server patching or matters corresponding to information security have been addressed accordingly, but these should be implemented in a more thorough manner.

REFERENCES

[1] E. H. Arthur, S. Bosworth and D. B. Hoyt. (1995). Computer Security Handbook. New York: John Wiley & Sons 1995.

[2] K. P. Badenhorst and J. H. P. Elloff. Framework of a Methodology for the Life Cycle of Computer Security in an Organization. Computer & Security, 8:5 (1989), 433-442.

[3] A. Christophy and A. Dorofee. Introduction to the OCTAVE Method. The CERT® Coordination Center (CERT/CC) 2001).

[4] R. J. Ellison, R. C. Linger, T. Longstaff and N. R. Mead. Survivable Network System Analysis: A Case Study. IEEE Software, 16:4 (1999), 70-77.

[5] J. H. P. Eloff and M. M. Eloff. Information security architecture. Computer Fraud & Security, 11 (2005), 10-16.

[6] M. M. Eloff and S. H. Von Sloms. Information Security Management: A Hierarchical Framework for Various Approaches. Computers & Security, 19:3 (2000), 243-256.

[7] M. M. Eloff and S. H. Von Sloms. Information Security Management: An approach to Combine Process Certification and Product Evaluation. Computers & Security, 19:8 (2000), 698-709.

[8] J. E. Ettinger. "Key Issues in Information Security. Information Security 1993, Chapman & Hall, London, 1-10.

[9] T. Finne. Information Systems Risk Management: Key Concepts and Business Processes, Computers & Security, 19:3 (2000), 234-247.

[10] M. Gehrke, A. Pfitzmann and K. Rannenberg. Information Technology Security Evaluation Criteria (ITSEC)-A Contribution to Vulnerability?. Proceedings of IFIP 12th World Computer Congress Madrld on Information Processing 1992, 7-11.

[11] D. Gollmann. Computer Security. John Wiley & Sons Ltd (UK) 1999.

[12] M. Gupta, A. R. Chartuvedi, S. Metha and L. Valeri. The Experimental Analysis of Information Security

Management Issues for Online Financial Services. Proceedings of the 2001 International Conference on Information systems, 667-675.

[13] S. Halliday, K. Badenhorst and R. Von Solms. A business approach to effective information technology risk analysis and management. Information Management &Computer Security, 4:1 (1996), 19-31.

[14] ISO/IEC 17799. Information technology-code of practice for information security management. BSI (London) 2000.

[15] L. J. Janczewski and F. X. Shi. Development of Information Security Baselines for Healthcare Information Systems in New Zealand. Computer & Security, 21:2 (2002), 172-192.

[16] E. E. Schultz, R. W. Proctor and M. C. Lien. Usability and Security An Appraisal of Usability Issues in Information Security Methods. Computers & Security, 20:7 (2001), 620-634.

[17] J. Sherwood. SALSA: A method for developing the enterprise security architecture and Strategy. Computer & Security, 2:3 (1996), 8-17.

[18] E. Smith and J. H. P. Eloff. Security in health-care information systems-current trends. International Journal of Medical Informatics, 54 (1999), 39-54.

[19] M. J. Song. Risk Management. Chinese Enterprise Develop Center 1993, 33-456.

[20] D. Trcek. An Integral Framework for Information Systems Security Management. Computers & Security, 22:4 (2003), 337-360.

[21] R. Von Solms. Information Security Management: The Second Generation. Computer & Security, 15:4 (1996), 281-288.

[22] R. Von Solms, H. Van Haar, S. H. Von Solms and W. J Caelli. A Framework for Information Security Evaluation. Information & Management, 26 (1994), 143-153.

[23] A. H. Willet. The Economic Theory of Risk and Insurance. Ph. D. Thesis in Columbia University, 1901.

Kuo-Hsiung Liao is a lecture of Information Management at the Yuanpei University, HsingChu, Taiwan. He received the M.S. degree in computer science from the New York Institute of Technology in 1992. He has published papers in the fields of e-government, and medical information management. His research interests include neural networks, computer security, programming language, artificial intelligent, medical information management and pattern recognition.

Hao-En Chueh is an assistant professor of Information Management at the Yuanpei University, HsingChu, Taiwan. He received the Ph.D. in Computer Science and Information Engineering from Tamkang University, Taiwan, in 2007. His research areas include data dining, fuzzy set theory, probability theory, statistics, database system and its applications, etc. He is now the Editor In Chief of International journal of Web & Semantic Technology (IJWesT).