Using the Balanced Scorecard to Evaluate the Value of Information Assets in Security Risk Management of Medical Care

Bo-Jie Juang & Hung-Wei Lin
Institute of Healthcare Information Management
National Chung Cheng University, Taiwan
168,University Rd, Min-Hsiung Chia-Yi, Taiwan, R.O.C.
TEL: 886-5-2721500, FAX: 886-5-2721501
Sam.liondance@gmail.com

Abstract: Information technology has been widely applied in the fields of globally medical care, which makes the service apparently progress in its quality and efficiency. However, medical information that was stored in electronic form really causes the risk of leaking.

A good security risk management offers a positive guarantee for hospitals, which highly relying on information technology, while running their organization.

While carrying out risk analysis, the value of information assets, existing weakness, and potential threat from outside of this information system must be realized. It is quite important to determine the value of information assets for the security risk management.

With information age coming, there is the greater part of asset value not shown from the traditional balance sheets in accounting books. This kind of asset, which can't be shown on the balance sheet, is intellectual capital. In the study of information asset and intellectual capital, Ross et al. (1996) divided information assets into three kinds of capitals - human asset, technology asset and relationship asset. These play the same tune with the three key elements of intellectual capitals- human capital, structural capital and relational capital. Within numerous assessment methods of intellectual capital, balanced scorecard assesses intellectual capital value from the view of management and efficiency.

Hence, this research proposes utilizing the balanced scorecard to find out the assessment index of information assets for domestic medical institutes while carrying on risk management. Hopefully, the results of this research can be regarded as the references of risk management of information security for domestic medical institutes.

Keywords: Internet Security and Privacy.

I. Introduction

Hospitals are indispensable in the social, and undertake the first line rescue of health and safety. Therefore, there are many hospital requests that come from the law and the society from all walks of life. The biggest difference between hospitals and other professions service is that medical service matters person's health and the life and death. A slight mistake or a fault may bring about a regret that is irrevocable or unable to make up. Therefore, hospitals and other general organizations have the enormous difference in the processing service and decision-making.

Information technology has been widely applied in the fields of globally medical care, which makes the service apparently progress in its quality and efficiency. However, medical information that was stored in electronic form really causes the risk of leaking. That's why people care most about rights of privacy after the electronic medical record was brought into practice. Also, legislation and the promotion of electronic medical record are influenced by this factor but not problems from technology（Dye, 1986; Hall & Rich, 2000）.

The United States formulated HIPAA (Health Insurance Portability and Accountability Act) in 1996.It was from the legal stratification plane to establish the right of privacy protection standard that can be observed by hospitals. In Taiwan, The Department of Health (DOH) has established a working group of "the medical information security and the privacy protection guiding principles" in order to strengthen patients' medical information security and the privacy protection. The working group has drafted "the medical information security and the privacy protection guiding principle".

After looking at the domestic and foreign laws and regulations, it can be understood that information security is very important for hospitals. The overseas government and the medical system none who does not devote to patients' electronic data security and the privacy protection hoped to formulate each kind of laws and regulations to make the medical system observe the protection standard. Because of the laws and regulations restrictions, hospitals must start to plan ISMS for each information security request. Risk management plays a critical role in protecting an organization's information assets. An effective risk management process is an important component of a successful IT security program. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization.（Stoneburner, G., A. Goguen, et al., 2002）.

Risk management includes two major parts - risk analysis and risk control (Boehm, 1991). While carrying out risk analysis, the value of information assets, existing weakness, and potential threat from outside of this

Proceedings of the Fifth International Conference on Electronic Business, Hong Kong, December 5-9, 2005, pp. 457 - 462.

information system must be realized. It is quite important to determine the value of information assets for the security risk management, because the more indefinite the value of information assets in the organization is, the harder to realize which asset is so worthy and important that needs special protection or even being reduced or shifted its risk; or, with limited resources, the risk is acceptable because the value of the asset is low. Besides, managers of the organizations often rely on the value of the assets to determine the investment of information security. Now, there is not a standard measurement index to assess the value of information assets in the relevant information security management standards.

Hence, this research proposes utilizing the balanced scorecard to find out the indicators of information assets assessment for domestic medical institutes while carrying on risk management. The importance of each kind of information assets must be confirmed through the assessment indicators. The results of this research can be regarded as the references of risk management of information security for domestic medical institutes.

II. Information Security

The so-called information security is to apply the management and the technology to hardware, software and data. It avoided other people to read, add, delete and modify storing or transmitting data. The rigorous level of information security management and the precise level of technology were decided by the risk which information was exposed under the procedure or the technique.

Other definitions of information security were collected in table 1:

Table 1、The Definition of Information Security

Name	Year	Content
Eloff and von Solms	2000	Data or information system still conforms to the security demand after passing through a series of test.
Finne	1997	Information security means a number of measures taken to minimize the risks connected to information.
Schultz, Proctor, Lien and Salvendy	2001	Information security in its most basic sense is protecting computer-related assets such as computers, networks, data, programs, and the hardware components.
Parker	1997	Information security is concerned with information protection that includes individual conversation, printing files and automated records.

（Source：My reorganization）

Icove (1,995) thought that the generalized computer security contained several constructions:

- **Physical Security**：the protection of computer facility. Physical security avoids stealing and destruction of these facilities. Physical security also guarantees the computer facility against the natural disaster and all damage that is made by other environmental factor.
- **Personnel Security**：personnel security covers widespread scope, promoting computer security is one goal of strengthening personnel security. The goal of personnel security is to prevent personnel's security threat. It is an important part of personnel security to investigate personnel's background and monitor the operations.
- **Communication and Data Security**：the goal of communication and data security is to protect data transmission security ,including mail, telecommunication, facsimile and Internet. Internet is in fashion; communication and data security already became one of projects that the enterprise should specially pay great attention to.
- **Operations Security**：the goal of operations security is to prevent the compute crime, and raise attention to the computer crime.

The following figure shows the concept of computer security that was proposed by Carroll.

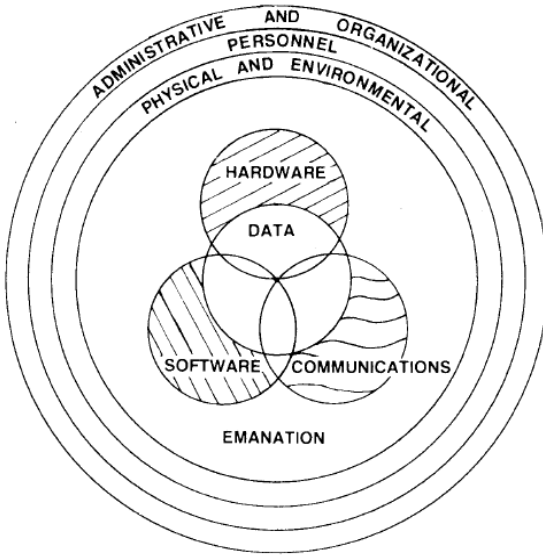

Figure 1、The Concept of Computer Security（Carroll,1987）

The technical tradition security concerning IT and information is typically defined by three aspects; confidentiality, integrity and availability（Gollman, 1999; Harris, 2002; Jonsson, 1995）.

Gollman (1999) define CIA as follows:

- **Confidentiality:** Prevention of unauthorized disclosure or use of computer systems and data
- **Integrity:** Prevention of unauthorized modification of computer systems and data
- **Availability:** Ensuring authorized access of computer systems and data when required

The definition of information security management which was proposed by Russell and Gangemi (1992) is that, "The information security management is to protect all things related with computer security, including computer, software, data, terminals, printers, tapes, disks, even the computer rooms." Consequently the managing of

information security should differ between organizations (Mintzberg 1983, Baskerville 1993).

Various authors (e.g., Siponen and Baskerville, 2001; Straub and Welke, 1998; Baskerville, 1993, Hitchings, 1995) suggest that the major problem with current approaches to managing IS security relates to the technical orientation of the solutions. They argue that the social and organizational aspects should be more considered in managing information security.

A good security risk management offers a positive guarantee for hospitals, which highly relying on information technology, while running their organization.

There is a discussion of the hospital information security problems in the following section. The first hospital information security problem is about internal personnel. Before computerizing, patient records in paper form had to prevent the natural disaster and stealing. Although now electronic patient record has been developed. It is still a big threat for internal personnel stealing.（Ross, 1996）

Software bugs and hardware failures occasionally corrupt messages. While mail, fax and telephone systems also fail, their failure modes are more evident than those of computer messaging systems. With poorly designed software, the figure could be substantially higher.（Ross, 1996）

Viruses have already destroyed clinical information, and a virus could conceivably be written to make malicious alterations to records.（Ross, 1996）

A malicious attacker might also manipulate messages. Sending email, which appears to come from someone else, is easy, and with some more effort it is possible to intercept mail between two users and modify it.（Ross, 1996）

By the literature, information security actually works in many ways, it involves technology, management even involves to policy, and legislation and so on, if everything get prepare in advance, many persecutions might be eliminated in the future.

III. Security Risk Management

Each industry has its unique commercial risk. In medical care industries, the commercial risk is patient safety, PHI and the right of privacy. Therefore, hospitals need the risk management. Besides IT risk assessment, hospitals also need the enterprise risk assessment to guarantee each person's responsibility.（Louis J. Carpenito, 2004）

Once the enterprise decides to establish the ISMS, the steps of risk management are inevitable. Generally speaking, the steps of risk management may be divided into the following four steps.

I. Identification and Recognition
II. Measurement and Evaluation
III. Selection Risk Management Techniques
IV. Implementing and Evaluation

Proper risk assessment planning is critical to the success of the entire risk management program. Assessing risk requires cross-group interaction and for different stakeholders to be held responsible for tasks throughout the process. A best practice to reduce role confusion throughout the process is to communicate the checks and balances built into the risk management roles and responsibilities. While you are conducting the assessment, communicate the roles that stakeholders play and assure them the Security Risk Management Team respects these boundaries. The following table summarizes the roles and primary responsibilities for stakeholders in this phase of the risk management process.

Table 2、Roles and Responsibilities in the Risk Management Program

Role	Responsibility
Business Owner	Determines value of business assets
Information Security Group	Determines probability of impact on business assets
Information Technology--Engineering	Designs technical solutions and estimates engineering costs
Information Technology--Operations	Designs operational components of solution and estimates operating costs

（Source：The Security Risk Management Guide）

Business Owners have explicit roles in the risk assessment process. They are responsible for identifying their organizational assets and estimating the costs of potential impacts to those assets. Most information security professionals and non – technical stakeholders do not realize this connection automatically. Business managers often rely on the value of an asset to guide them in determining how much money and time they should spend securing it. At present, the methods of estimating the value of information assets are subjective. No objective tools or methods for determining the value of an asset exist.

IV. Information Assets and Value Estimate

The enterprise assets may be tangible or intangible. Both needs to be defined explicitly, business owner can explicitly estimate the value. The value of information assets is based on the impact degree to the organization. From the viewpoint of information security, the asset classification and the control are so important in the risk assessment.

The IT service combined tangible assets with intangible assets. Organization can first handle the most essential assets after the information asset classification has been done. Generally speaking, the information assets can be divided into five categories. The proportions of these five categories are not the same in different business projects, workflows, organization characteristics and culture.（Alberts, et al., 2003）

Security requirements outline the qualities of information assets that are important to an organization.

When the security requirements of an asset are violated, certain outcomes are possible (outcomes are directly related to security requirements in the table below).

Table 3、Relationship of Security Requirements to Outcomes

Security Requirement	Outcome
Confidentiality	● Disclosure of asset
Integrity	● Modification of asset
Availability	● Destruction of asset ● Loss of asset ● Interruption of asset

（Source：Health Information Risk Assessment and Management）

Asset values are based on the impact to the organization if the asset is lost. For some tangible assets, standard accounting procedures or replacement costs can be used. Acquired value for intangible assets can be estimated based on the loss to the enterprise.（Hutt, et al., 1995）The traditional measure of an asset is in terms of dollars. Reducing all assets to dollars makes for an easy comparison, and people are often comfortable thinking in terms of dollar values for assets. It can be very difficult, however, to reduce some intangible assets to dollar values. The cost of estimating statistically can be high in some cases, and statistical estimates may depend on subjective assumptions. Historical data, if available, can be useful in estimating the value of assets. In many cases relative rankings of asset values are sufficient.（Fites, et al., 1989）One way to estimate the value of assets is to consider what would happen if their security requirements were violated. Let's consider an example in which a medical center wants to protect its patient records. Staffs are concerned about the possibility of disclosing the patient records because this would violate the security requirement that sensitive information must remain confidential. If the information is disclosed to an unauthorized party, the fact that the information is no longer confidential has an impact on the organization. If the impact affects private medical diagnostic results or treatment plans, the value of the asset would be extremely high. On the other hand, disclosure of staffing assignments for nursing shifts, for example, might not have a serious impact on operations, so the asset value would be low.（Alberts, et al., 2003）

With information age coming, there is the greater part of asset value not shown from the traditional balance sheets in accounting books. This kind of asset, which can't be shown on the balance sheet, is intangible asset. It is also called intellectual capital. According to literature, intangible asset has taken the majority of the whole value in the software and IC industries.

The suggested measuring approaches for intangibles fall into at least four categories of measurement approaches. The categories are an extension of the classifications suggested by Luthy (1998) and Williams (2000).

- ✧ **Direct Intellectual Capital methods (DIC).**
- ✧ **Market Capitalization Methods (MCM).**
- ✧ **Return on Assets methods (ROA).**
- ✧ **Scorecard Methods (SC).**

The methods offer different advantages. The methods offering $-valuations, such as ROA and MCM methods are useful in merger & acquisition situations and for stock market valuations. They can also be used for comparisons between companies within the same industry and they are good for illustrating the financial value of Intangible assets, a feature, which tends to get the attention of the CEOs. Finally, because they build on long established accounting rules they are easily communicated in the accounting profession. Their disadvantages are that by translating everything into money terms they can be superficial. The ROA methods are very sensitive to interest rate and discounting rate assumptions and the methods that measure only on the organization level are of limited use for management purposes below board level. Several of them are of no use for non-profit organizations, internal departments and public sector organizations; this is particularly true of the MCM methods. The advantages of the DIS and SC methods are that they can create a more comprehensive picture of an organisation's health than financial metrics and that they can be easily applied at any level of an organisation. They measure closer to an event and reporting can therefore be faster and more accurate than pure financial measures. Since they do not need to measure in financial terms they are very useful for non-profit organisations, internal departments and public sector organisations and for environmental and social purposes. Their disadvantages are that the indicators are contextual and have to be customised for each organisation and each purpose, which makes comparisons very difficult. The methods are also new and not easily accepted by societies and managers who are used to see everything from a pure financial perspective. The comprehensive approaches can generate oceans of data, which are hard to analyse and to communicate.

In Scorecard methods, one method is balanced scorecard. It belongs to the non- dollar method. Kaplan & Norton proposed this method in 1992. They proposed the concept of balance scorecard because enterprise's performance measurement and the strategy management should not only consider the financial aspect in new environment. It is an ideal way to contain company's intangible asset. This may make up the insufficiency of financial accounting. This idea is the same as asset value estimate in security risk management.

Within numerous assessment methods of intellectual capital, balanced scorecard assesses intellectual capital value from the view of management and efficiency. Many enterprises declared that they had already applied the balanced scorecard. Its performance measurement has covered the finance and the non- finance index. Such system is more balanced than the financial system.

The balanced scorecard includes four constructions to measure organization performance. The concept of balanced scorecard is suitable for the value estimate of intangible assets.

The balanced scorecard is used in the healthcare

institutes initially, but some articles had described the use of balanced scorecard in the healthcare environment and its potential benefit.

The healthcare institutes that have used the balanced scorecard consider the difference between BSC and other systems:

- The majority of measuring approaches were only suitable in partial management, clinical and diagnostic functions.
- Other measuring approaches were unlike BSC to provide leading indicators.

BSC can be used to express the strategy complexity and the interaction relations through the linkage of causal relations. The information of cost, quality and workflow can be easily and clearly exchanged.

V. Conclusions and Future Work

The enterprise assets may be tangible or intangible. Both needs to be defined explicitly, business owner can explicitly estimate the value. The value of information assets is based on the impact degree to the organization. From the viewpoint of information security, the asset classification and the control are so important in the risk assessment. The traditional measure of an asset is in terms of dollars. But balanced scorecard is different to the traditional method. It belongs to the non- dollar method. The concept of balance scorecard is that enterprise's performance measurement and the strategy management should not only consider the financial aspect in new environment. It is an ideal way to contain company's intangible asset. This may make up the insufficiency of financial accounting. This idea is the same as asset value estimate in security risk management.

The balanced scorecard is used in the healthcare institutes initially, but some articles had described the use of balanced scorecard in the healthcare environment and its potential benefit. Hence, this research proposes utilizing the balanced scorecard to find out the indicators of information assets assessment for domestic medical institutes while carrying on risk management. The importance of each kind of information assets must be confirmed through the assessment indicators. And the results of this research can be regarded as the references of risk management of information security for domestic medical institutes. Hospitals can use security risk management to take appropriate control, to reduce, to prevent, and to change its commercial risk. Then the hospital operation could be continuing.

It is a convenient and effective solution to use the electronic medical information for improving the quality of medical service. Hospitals can avoid the repetition and the waste of medical resources. They can achieve the purpose of saving the medical cost through the connectivity and the exchange of the electronic medical information.

Although there are many merits for using the electronic medical information, however, it still has the information security problems such as data integrity, confidentiality, non-repudiation and identification. How to obtain the balance in reasonably using the electronic medical information and in protecting patients' privacy is a important issue that should be paid attention to when planning the electronic healthcare information service.

References

[1] Anderson RJ. *Security in clinical information systems*, London: British Medical Association, 1996.

[2] Baskerville, R. "Information systems security design methods: implications for information systems development." ***ACM Computing Surveys***, 1993, 25:375-414.

[3] Boehm, B. W. "Software risk management: principles and practices." *IEEE Software***,** 1991,32-41.

[4] Carroll, J.M. *Computer security***,** 2nd Ed, Butterworth-Heinemann, 1987.

[5] Dyer, C. "Disclosure of medical records in litigation." *British Medical Journal*, 1986,293:1298.

[6] Eloff, Mariki M. and Von Solms, Sebastiaan H. "Information security management: An approach to combine process certification and product evaluation." *Computers & Security***,** 2000, (19:8), 698-709.

[7] Finne, T. "A conceptual framework for information security management." *Computers & Security***,** 1997, (16:6), 469-479.

[8] Fites, Philip E.; Kratz, Martin P. J.; & Brebner, Alan F. *Control and Security of Computer Information Systems.* Rockville, MD: Computer Science Press, Inc, 1989.

[9] Gollman D. *Computer security*, Wiley, 1999.

[10] Hall, MA & Rich, SS. "Genetic privacy laws and patients' fear of discrimination by health insurers: The view from genetic counselors." *Journal of Law, Medicine & Ethics*, 2000, 28: 245-57.

[11] Harris S. *CISSP certification exam guide***,** McGraw-Hill/Osbourne, 2002.

[12] Hitching J. "Deficiencies of the traditional approach to information security and the requirements for a new methodology computers and security." 1995.

[13] Hutt, Authur E.; Bosworth, Seymour; & Hoyt, Douglas B. *Computer Security Handbook*, 3rd ed.New York, NY: John Wiley & Sons, Inc, 1995.

[14] Icove, David. , Seger, Karl. And VonStorch, William. "Computer crime: A crime fighter's handbook." 1st Ed, O'Reilly & Associates, Inc, 1995.

[15] Jonsson E. "A quantitative approach to computer security from a dependability perspective." Doctoral Dissertation, Department of Computer Engineering, Chalmers University of Technology, Göteborg, 1995.

[16] Louis J. Carpenito. **"**Implications of the HIPAA Security Rule." Available online: http://enterprisesecurity.symantec.com/industry/healthcare/article.cfm?articleid=3211, 2004.

[17] Luthy, D.H. "Intellectual capital and its measurement." Available Online: http://www3.bus.osaka-cu.ac.jp/apira98/archives/htmls/25.htm, 1998.

[18] Mintzberg, H. *Structures in fives: designing effective organizations*, Englewood Cliffs, NJ: Prentice-Hall, 1983.

[19] Parker, Donn B. "Information security in a nutshell." *Information Systems Security*, 1997, (6:1), 14-19.

[20] Russell D. and G. T. Gangemi. *Computer security basics*, O'Reilly & Associates, Inc, 1992.

[21] Schultz, E. Eugene. , Proctor, Robert W., Lien, Mei-Ching and Salvendy, Gavriel. "Usability and security: An appraisal of usability issues in information security methods." *Computers & Security***,** 2001, (20:7), 620-634.

[22] Siponen, M., and Baskerville, R. "A new paradigm for adding security into IS development methods." In advances in information security management & small systems security, 2001.

[23] Stoneburner, G., A. Goguen. "Risk management guide for information technology systems." Washington D.C., National Institute of Standards

and Technology, 2002.
[24] Straub, D. W., and Welke, R. J. “Coping with systems risks: security planning models for management decision making.” *MIS Quarterly*, 1998, 22:441-469.
[25] Williams M. “Is a company’s intellectual capital performance and intellectual capital disclosure practices related? Evidence from publicly listed companies from the FTSE 100.” Paper presented at McMasters Intellectual Capital Conference, Jan 2001 Toronto, 2000.