經營科學
第17卷 第1號
2000年 5月

The Recommendation of Controls for Hospital Information System Using CRAMM: Case Studies of Two Korean Hospitals

Song-Chul Moon* · In-Goo Han** · Sang-Jae Lee***

Abstract

The medical records of diagnostic and testing information include sensitive personal information that reveals some of the most intimate aspects of an individual's life. The hospital information system (HIS) operates in a state of high risk which may lead to the possible loss to the IS resources caused by various threats. This research addresses twofold: (1) to perform asset identification and valuation, and (2) to recommend countermeasures for secure HIS network using case studies. This paper applied a risk management tool, CRAMM (Central Computer and Telecommunications Agency's Risk Analysis and Management Method), to assess asset values and suggest countermeasures for the security of computerized medical information of two large hospitals in Korea. CRAMM countermeasures are recommended at the reference sites from the network security requirements of systems utilized for the diagnosis and treatment of patients. The results of the study will enhance the awareness of IS risk management by IS managers.

1. Introduction

Health care information and medical record are composed of sensitive personal information that is related to some of the most intimate aspects of an individuals life. This sort of information related to the medical record includes the details of a persons family story, genetic testing, history of diseases and treatments, and history of drug use. These data are considered to be crucial because health care information can influence decisions about an individuals access to credit, admission to educational institutions, and his/her ability to secure employment

* Systec Cop.
** Graduate School of Management Korea Advanced Institute of Science and Technology
*** Techno-Management Research Institute Korea Advanced Institute of Science and Technology

and obtain insurance [4]. Inaccuracy in the information or its improper disclosure can deny an individual access to these basic necessities of life, and can threaten an individuals personal and financial well-being. The efficiency of modern health care relies more and more upon a computerized infrastructure. Multimedia applications integrate formerly separated functionalities. But such technology may compromise the privacy of patients, and may subvert the accountability and secrecy of health care professionals [14]. Technologies to support communications of all kinds are evolving at an unprecedented rate. This transition of Integrated Services Digital Network (ISDN) to an all-digital network, when complete, will have wide-ranging implications for improving health care because it will open a new era for communication of all types of information, including that contained in the Computer based Patient Records (CPR) [6]. Internal and world-wide communication, access to medical databases, and information services are essential demands in the science of medicine not only for research, but also for improving patient care [13].

Patient privacy has been a concern of medical informatics since before most hospitals had ever seen a computer system. As of this date, the problem is still not solved. There appears to be an intractable conflict between the legal concept of data protection and the use of information in the modern computer environments, especially the use of information in networking [3, 22, 26]. The widespread of distributed systems in medical information systems and the functional structure of medical information systems have necessitated the implementation of network security [18]. Network security management will specify the required thing which should manage the secure framework in order to provide functional and efficient security [14].

The dependence on hospital information system and the recognition that hospital information is a vital source, require that management act to secure information resources. The important step, therefore, should be to make a decision to suggest countermeasures for security and integrity of IS resources (i.e., hardware, software, personnel). Such countermeasures allow organizations to attain a security level that fits its policy while meeting security requirements that represent the extent to which the information and resources are sensitive and critical to organizations.

The purpose of this study is: (1) to perform asset identification and valuation, and (2) to recommend countermeasures for secure HIS network using CRAMM (the Central Computer and Telecommunications Agency's Risk Analysis and Management Method) using case studies. This paper analyzes the implications of computerized medical information and the challenges that it brings to system security and individual privacy. The study shows asset valuation and countermeasure selection procedures against two hospital information systems. CRAMM countermeasures are recommended at the reference sites from the network security requirements of systems utilized for the diagnosis and treatment of patients. A summary of empirical findings, implications for practice, and future research issues are also

presented.

2. Security Management of HIS

Traditionally, information security has been considered to have three fundamental objectives: (1) *confidentiality* for ensuring that information is not disclosed or revealed to unauthorized persons; (2) *integrity* for ensuring consistency of data; in particular, preventing unauthorized creation, alteration, or destruction of data; (3) *availability*: ensuring that legitimate users are not unduly denied access to information and resources. The need for information security and trust in health care information computer systems, as in computer systems generally, can be described in terms of above three fundamental goals, confidentiality, integrity, availability [25]. Confidentiality involves control over who has access to information. Integrity assures that information and programs are changed only in a specified and authorized manner, that computer resources operate correctly and that they are not subject to unauthorized changes. A system meeting standards for availability allows authorized users access to information resources on an ongoing basis [21]. To support these objectives, management needs to have a security policy and needs to put in place a range of security measures to ensure that the goals of the security policy are met [9].

The level of security provided may vary from one application to another [17]. For example, security in computer systems containing classified national security information may have different specifications than a computer system designed for a nondefence manufacturing company. U.S. Congress, Office of Technology Assessment (OTA) indicated that an individual system may sacrifice the level of one requirement to obtain a greater degree of another [17, 18]. For example to allow for increased levels of availability of information, standards for confidentiality may be lowered. Thus, the specific requirements and controls for information security can vary. Applications linked to external systems will usually require different security controls from those without such connections because access is more open [22, 29]. The emphasis given to each of the three requirements (confidentiality, integrity, availability) depends on the nature of the application. Security in health care information systems would likely be designed to meet reasonably the three requirements.

The efficiency of modern health care relies more and more upon a computerized infrastructure. Multimedia applications integrate formerly separated funtionalities. On the one hand, easy processing and communication of images, sounds, and texts will help to represent illnesses and diseases holistically. But on the other hand, such technology may compromise the privacy of patients, and may subvert the accountability and professional secrecy of health care professionals. The European Union has initiated a multi-disciplinary project to come up with practical guidelines on how to achieve a secure Environment for Information Systems in MEDicine (SEISMED). SEISMED suggests that it is the decision of the management in charge of an IT-system to decide what the relevant threats to HIS are. Risk analysis is conducted to

observe the vulnerabilities of an IT-system with respect to the anticipated threats. Experiences with the risk analysis of existing systems are helpful for the design of new IT-systems as well [14].

The technical countermeasure should address both the secure upgrade of existing operational IT-systems and the design and development of new ones. For sensitive medical data, conventional security mechanisms such as passwords are insufficient. A separate guideline on cryptography, for instance, recommends mechanisms basically for authentication and encipherment purposes. Further, it needs to appraise the medical requirements and arrive at "practical" guidelines. The organizational and technical recommendations of the high-level security policy are made more precise by the guidelines on system development and on existing systems. For instance, the security requirements in both digital networks and databases are made more precise by the guideline on cryptographic mechanisms.

There are four basic approaches to security [8]: (1) to invest in all the security devices that are available, (2) habitually to react to the latest scare, (3) to patch up the holes as they appear, (4) to carry out a risk management exercise. The fourth risk management approach is a systematic method of assessing the risks and then applying the countermeasures where there is apparently the greatest need. It is an empirical rather than a scientific process and usually involves a series of value judgments which are then treated in such a way as to arrive at a risk assessment. Countermeasures are applied in accordance with the severity of the risk.

Risk analysis and risk management is interrelated process for IS security [30, 31]. Risk analysis is the identification and assessment of the measure of risks [23]. Risk is assessed from the assessed values of assets and the assessed levels of threats and vulnerabilities [12]. Risk management is identification and selection of countermeasures by the identified assets, threat, vulnerability, and risks. To clearly describe risk management, the definitions of several key terms are needed. Risk is defined as "the probability of loss or injury" [15]. Asset is everything and everybody who forms, or will form, part of the system operation.

A threat is a person, thing, event, or idea which poses some danger to an asset, in terms of that asset's confidentiality, integrity, availability, or legitimate use [16, 27]. Threats include actions and events which may jeopardize the objectives of the system. Vulnerability means a weakness which allows a threat to cause an undesirable impact. Impact indicates the effects of a threat occurrence on the system. Vulnerabilities are weakness in a safeguard, or the absence of a safeguard. Risk is high if the value of a vulnerable asset is high, and a probability of a successful attack is high. Conversely, risk is low if the value of the vulnerable asset is low and provability of a successful attack is low. Countermeasure is a control, mechanism, or procedure that protects an asset from threats.

Originators of existing computer-based patient record systems have been faced with the problem of ensuring that their systems will provide high levels of clinical access and utility for their personnel and still maintain the se-

curity and confidentiality of patient information [1, 11, 24]. Data security and confidentiality remain a central concern as the health care industry contemplates full automation and implementation of a networked computer system for individual health care information [6].

3. Use of CRAMM

A risk management method must be able to deal with operational and administrative systems of all sizes and to encompass all technical (e.g., software, communications) and non-technical (physical, personnel etc.) aspects of Information technology (IT) security [19]. There are a number of software products available, among them MARION (marketed by Coopers and Lybrand, Deloitte), Riskpac (of Computer Security Ltd.) and CRAMM (developed for CCTA and sold for them through a number of agencies) [5, 20]. The general approach of software product is similar in all products. The method should be compatible with existing government IT security guidance and suitable for use during the development of a system. Further, it should be easy to be used by staff with IT experience but not necessarily IT security experience [28]. In addition, the method should be able to be used in such a way that reviews can be carried out quickly. The method should be able to present results in a form which is readily understandable to non-technical general management [5, 10].

The risk management method used in this study is based on CRAMM. The CRAMM software enables a security review to complete a risk management of an information technology (IT). CCTA is the department within Her Majestys Government (HMG) responsible for the development of CRAMM. The method enables a complete security review of a current or projected IT system to be undertaken covering all aspects of security [2].

4. Case Studies

Y and S Hospital were selected as cases of the study. These hospitals have more than 500 beds. The data used in this research were obtained by using structured interview with IS staff members. The questionnaire instruments generated by CRAMM are made to identify assets and assess asset values along with overall state of HIS security, possibility and impact of violation of confidentiality, integrity, availability, and possibility and impact of interception risk, interruption risk, modification risk, fabrication risk.

CRAMM is applied to Y Hospital and S hospital to show risk management procedures for HIS. Countermeasures of network security are suggested through the tool of risk analysis, CRAMM. CRAMM had previously been utilized in a number of UK hospitals and it provided a stable basis for measuring security requirements across national boundaries. An examination of the detailed CRAMM countermeasures could recommend that the security requirements of systems utilized for the diagnosis and treatment of patients would demand much higher levels of security than had previously been contemplated.

The CRAMM training course provides a vital introduction to the principles of CRAMM to-

gether with practical guidance on the activities involved with the use of the CRAMM Software. The requirement to provide the means to undertake rigorous reviews can lead to the inexperienced user collecting excessive amounts of data. The intended use of CRAMM should be carefully scoped at the commencement of the review to ensure that resources are not wasted.

4.1 Y Hospital

Using CRAMM, assets are identified and valued in this study. The countermeasures to reduce each of the potential impacts of disclosure, modification, unavailability and destruction are identified. The recommendation of countermeasures is concerned with managing the risks to the system by establishing the countermeasures needed to meet the risks.

The classifications of physical assets of Y Hospital are indicated in <Table 1> following the classification criteria of CRAMM. Physical assets are divided into three parts, hardware, communication, and environment. Hardware consists of CPU, storage device, I/O device, network processor, and personal computer. Communication assets include LAN, WAN, internal communication equipments. The descriptions of three classifications of physical assets are represented in <Table 1.>

Asset valuation is the identification of assets that compromise the system and their valuation in terms of the possible impacts on them of disclosure, modification, unavailability and destruction. These assets may be physical, software, and data assets. Physical assets are valued based on the replacement and reconstruction cost of the individual asset. Namely, asset value is the sum of acquisition cost and capital expenditure (not considering revenue expenditure) minus depreciation expense. The valuations of physical assets are represented in <Table 2>. The values of software assets are

〈Table 1〉 Classification of Y Hospital Physical Asset

Class	Sub-class	Type	Asset name
Hardware	CPU	Multi-user Microcomputer	
	Storage Device	Disk Drive	Server
		Tape Drive	Extrabyte
	I/O Device	Remote Intelligent Terminal	CD 3.5" FDD
		Printer	Qnix Laser
	Network Processor	Intelligent Network Controller	Emulator
	Personal Computer		PC
Communi-cation	LAN Equipment	Ethernet	LAN Card
	WAN Equipment	Modem	WAN Modem
	Internal Communication	Inter-Processor Link	Gateway, Bridge
		Terminal Link	HUB
Environ-ment		Air conditioning	Etc.1
		Power	Etc.2
		Water	Etc.3

〈Table 2〉 Valuation of Physical Assets of Y Hospital

Physical Assets	Value (Pound)
C. P. U.	162,601
Storage Devices	81,300
Input/output Devices	8,130
Network Processors	6,000
Personal Computers	1,219,512
LAN Equipment	813,008
WAN Equipment	40,650
Internal Communications	1,620,016
WAN Services	81,300
Environmental	81,300
Documentation	8,130

24,790 and 16,260 pounds for system and application software respectively. These figures are estimates of asset values rather than accurate values.

The above asset values provide auditors or management with guidelines regarding which components of hardware are absolutely essential to processing operations of the HIS. For instance, C.P.U., personal computers, and internal communications have the highest asset values, and countermeasures should be established to ensure the security of these assets. Determinations of real asset value to organizations should be made as to the degree of sensitivity, the need to know or need to access, and for data assets, the number of copies and the distribution requirements. The dollar values of software and data assets are difficult to quantify. That is, the direct replacements costs and losses an organization may incur if its program files and data are lost or destroyed.

Once the security need has been established for each asset group, the appropriate security measures to protect those asset groups against the relevant impacts must be established. CRAMM countermeasure database have 53 countermeasure groups. The results of countermeasure recommendation are based on CRAMM output using the data collected from study interview. A security measure group consists of a number of security measures that deal with the same threats. These security measure groups are split into the various security aspects (e.g., those security measures which act in the same fashion (procedural, physical)). Each group is further sub-divided into subgroups. From these analyses, CRAMM suggests various countermeasure groups. The countermeasure for network security of HIS of Y Hospital are composed of eight countermeasure groups:

(1) LAN resilience for network security of HIS: This is important procedures for remote activation of network management facilities (e.g. loopback, link disable).
(2) LAN protection for network security of HIS: Formal mandatory multi-level security to provide local area networks security devices.
(3) WAN resilience for network security of HIS: This includes important procedures to ensure that users are effectively apportioned between distribution frames and network interface points.
(4) WAN protection for network security of HIS: Regular inspections of junction boxes and distribution frames for wiretaps are demanded.
(5) Fire protection for network security of HIS: In order to protect assets from fire, automatic fire suppression should be prepared with manual override and separate main power supply.
(6) Water protection for network security of HIS: It is necessary to regularly check that the integrity of water tight floor voids has not been destroyed by apertures for cabling and ducting.
(7) Disaster protection for network security of HIS: Where replacement critical assets are held, these should be located in a physically remote area from those assets for which they are held as replacements.
(8) Service continuation for network security of HIS: For installations to which access

〈Table 3〉 Countermeasure Groups of LAN Resilience and LAN Protection for Hospital Y

Countermeasure Group	Security Aspect	Major Control Issues	Detail Countermeasures
LAN Resilience	Communication	Failure recovery	○ Alternative carrier routing ○ Dynamic alternative routing ○ Duplicate controllers with automatic changeover ○ Automatic reconfiguration around a cable break(LAN)
		Detection	○ Network monitoring equipment to detect circuit and equipment failure
		LAN protection	○ Remote activation of network management facilities (e.g., loopback, link disable) ○ Network redundancy --- redundancy capacity ○ Redundant routing ○ Redundant key components ○ Cabling protected against electromagnetic interference, fire, water etc. ○ Cabling protected against inadvertent physical interference ○ Software protection, and back-up, for network control information (e.g., routing tables) ○ Protection of routing tables during distribution to nodes
		Transmission protection	○ Facilities to prevent replay, e.g. message authentication and sequence checks ○ Facilities to prevent disclosure, e.g. encryption ○ Facilities for non repudiation ○ Facilities to ensure identity of remote user (e.g., port protection)
	procedural	LAN usage monitoring	○ Monitor volumes for over-utilization
		Testing procedures	○ Procedures for testing correctness of communications software and routing tables, in network management center and nodes
LAN Protection	communications	Data Integrity	○ Message authentication devices for financially related and other sensitive data transmission
		Data Confidentiality	○ Encryption of passwords transmitted over communications lines ○ Fiber optic cable ○ Monitor fiber optic signal strength for interference to detect unauthorized insertion or removal of equipment ○ Encryption devices ○ For local area networks security devices to provide formal mandatory multi-level security ○ Secure gateways LAN:LAN, LAN:WAN etc. ○ End to end encryption facilities
	procedural	Data integrity procedures	○ Procedures for start-up and close-down of non encrypted lines
		Data Confidentiality procedures	○ Key management and distribution procedures for encryption ○ Procedures for start-up and close-down of encrypted circuits ○ Procedures for time scheduling

may be denied by external events, necessary contingency planning should be prepared.

These eight countermeasure groups have detail countermeasures. For instance, the countermeasure group "LAN Resilience" and "LAN Protection" have various detail countermeasures as shown in <Table 3>.

4.2 S Hospital

The HIS of S hospital is operated by medical information team. Medical information team consists of department of operating and department of development. S Hospital uses Local

Area Network (LAN) to connect the hospital buildings of different site. The HIS of S Hospital is composed of mini-computer systems on the head office, and managed through AT&T UNIX server system. The classifications of physical assets of S Hospital are shown in <Table 4>. The classifications of physical are the same as those of hospital Y.

〈Table 4〉 Classification of S Hospital Physical Asset

Class	Sub-class	Type	Asset name
Hard ware	CPU	Mini-computer	AT&T UNIX NCR 3600
	Storage Device	Disk Drive	Server
		Tape Drive	Extrabyte
	I/O Device	Remote Intelligent Terminal	CD 3.5" FDD
		Printer	Unisys HART-8800LP
	Network Processor	Intelligent Network Controller	AT&T UNIX NCR 3600
	Personal Computer		PC
Communi-cation	LAN Equipment	Ethernet	LAN Card
	WAN Equipment	Modem	WAN Modem
	Internal Communication	Inter-Processor Link	Gateway, Bridge
		Terminal Link	HUB
Environ-ment		Air conditioning	Etc.1
		Power	Etc.2
		Water	Etc.3

In contrast with the case hospital Y, classification and valuation of software and data assets are performed for hospital S to preliminarily examine the software and data assets the values of which are difficult to assess. Software assets are divided two parts according to CRAMM criteria, system software and application software. Private data assets are classified into five data asset groups.

The results of asset assessment or valuation

〈Table 5〉 Classification of S Hospital Software Asset

Application S/W	descriptions
order communication system	management of foreign patient management of admission to a hospital management of patient inspection management of patient operation
office automation system	management of material & inventory management of personnel management of payroll
picture archiving and communication system	management of picture transmission
telemedicine system	management of telemedicine

〈Table 6〉 Classification of S Hospital Data Asset

Data Asset Group #	Descriptions
Data 1	Patient #, Password
Data 2	Patient #, Password, User Id
Data 3	Patient #, Password, User Id, Name, Association #
Data 4	Patient #, Password, User Id, Name, Association #, Physician #
Data 5	Patient #, Password, User Id, Name, Association #, Physician #, Department #

are suggested in <Table 7, 8, 9>. Physical assets are quantitatively valued based on the replacement and reconstruction cost of the individual asset. Namely, asset value is the sum of acquisition cost and capital expenditure (no considering revenue expenditure) minus depreciation expense. In contrast with hospital Y, the valuations of asset were conducted by interviewing the managers, operator of particular assets, or others who could speak authoritatively about the asset [7]. The values of software assets are 772,357 and 40,650 pounds for system and application software respectively. Further, the asset valuations of software and data assets are assessed qualitatively, as it is very difficult to value them accurately in a quantitative manner. The qual tative asset value has an ordinal value from 0 (*Very Low*) to 5

〈Table 7〉 Valuation of Physical Assets of S Hospital

(a) In quantitative value

Physical Assets	Value (Pound)
C. P. U.	1,919,690
Storage Devices	95,300
Input/output Devices	10,530
Network Processors	7,000
Personal Computers	2,951,219
LAN Equipment	1,138,762
WAN Equipment	67,750
Internal Communications	1,950,020
WAN Services	95,500
Environmental	93,800
Documentation	9,410

(b) In qualitative value

Physical Assets	Unavail-ability			Destruc-tion	Disclo-sure		Modifi-cation	
	I	S	D		S*	O	A	D*
CPU	1	2	4	5	1	1	2	2
Storage Devices	1	2	4	5	1	1	2	2
In/Out Device.	1	2	4	5	1	1	2	2
N/W Processor.	1	2	4	5	1	1	2	2
P/C	1	2	4	5	1	1	2	2
LAN Equipment	1	2	4	5	1	1	2	2
WAN Equipment	1	2	4	5	1	1	2	2
Internal Communication	1	2	4	5	1	1	2	2

I: Inconvenient, S: Serious, D: Disastrous, S: Staff, O: Outsiders, A: Accidental, D: Deliberate

〈Table 8〉 Assessment of Software Assets of S Hospital (In qualitative value)

Software Assets	Unavail-ability			Destruc-tion	Disclo-sure		Modifi-cation	
	I	S	D		S*	O	A	D*
S/W	1	2	4	5	1	0	2	0

I: Inconvenient, S: Serious, D: Disastrous, S: Staff, O: Outsiders, A: Accidental, D: Deliberate

(*Very High*) reflecting the impact of the loss of assets or the impact of various threats. The four types of impact considered in CRAMM are destruction, unavailability (inconvenient, serious, disastrous), disclosure (to staff or outsiders), modification (accidental or deliberate). The main calculation performed in CRAMM includes the assessment of these eight impacts (or threats). The ordinal values represent qualitative asset values or importance to business and cost of shutdown. For instance, the threat of destruction has the largest impact (5) on CPU than the other threats of unavailability, disclosure, and modification. The impact of threats is not different across different physical assets, indicating that threats affect these assets in a collective manner.

〈Table 9〉 Assessment of Data Assets of S Hospital (In qualitative value)

Data Assets	Unavail-ability			Destruc-tion	Disclo-sure		Modifi-cation	
	I	S	D		S*	O	A	D*
Data	1	2	4	5	1	0	2	0

I: Inconvenient, S: Serious, D: Disastrous, S: Staff, O: Outsiders, A: Accidental, D: Deliberate

Once the assets have been valued, the countermeasures for system can be established. There are eight countermeasure groups for network security of HIS of S Hospital:

(1) LAN resilience for network security of HIS: Cables (e.g., routing tables) should be protected from inadvertent physical interference, and software protection, back-up, for the security of network control information.
(2) LAN protection for network security of HIS: Internal cables should either be visible for inspection, or in sealed ducts for their whole length.
(3) WAN resilience for network security of HIS: this is important for testing the

correctness of communications software and routing tables in network management center and nodes.

(4) WAN protection for network security of HIS: Telephone numbers should be changed regularly and dial-up using private circuits should be disallowed during dial-up communications.

(5) Fire protection for network security of HIS: An effective and efficient procedure should be established to ensure that all persons, including visitors and temporary workers, can be prepared for an emergency like fire.

(6) Water protection for network security of HIS: Physical protection procedures

〈Table 10〉 Countermeasure Groups of LAN Resilience and LAN Protection for Hospital S

Countermeasure Group	Security Aspect	Major Control Issues	Detail Countermeasures
LAN Resilience	Communication	Failure recovery	○ Manual alternative routing
		Detection	○ Network monitoring equipment to detect circuit and equipment failure ○ Fault location notification
		LAN protection	○ Network redundancy --- redundancy capacity ○ Redundant routing ○ Cabling protected against inadvertent physical interference ○ Software protection, and back-up, for network control information (e.g., routing tables) ○ Protection of routing tables during distribution to nodes
	procedural	LAN usage monitoring	○ Monitor volumes for over-utilization
		Testing procedures	○ Procedures for testing correctness of communications ○ Software and routing tables, in network management ○ center and nodes
LAN Protection	communications	Data Integrity	○ Message authentication devices for financially related and other sensitive data transmission
	procedural	Data integrity procedures	○ Procedures for start-up and close-down of non encrypted lines
		Data confidentiality procedures	○ Procedures for start-up and close-down of encrypted circuits ○ Procedures for the use of specialized equipment (e.g., circuit testers, data analyzers, patching equipment and datascopes)
		Dial up protection procedures	○ Dial -up connection will only take place after a successful dial back ○ The line will be disconnected when not in use
		LAN usage monitoring	○ Procedures for the investigation of illegal attempts to access communications facilities
	physical	LAN protection	○ Physically protect cables from wiretapping, and connection of alien devices ○ Internal cables either visible for inspection, or in sealed ducts for their whole length ○ Inspection by guards, under direction of the Security officer ○ Guards provided with a plan annotated with connection points and whether a device should be attached or not ○ Physically protect distribution frames and junction boxes for the same reason ○ Underground routing of external cables to discourage wiretapping or illegal insertion of devices ○ Communications circuit lock or cable disconnect ○ Physical protection of encryption devices ○ Physical protection of key material for encryption devices ○ Physical safekeeping of specialized equipment (e.g., circuit testers, data analyzers, patching equipment and datascopes)

should ensure that under-floor cabling, junction boxes, etc. should be water-proofed.

(7) Disaster protection for network security of HIS: As far as possible all critical assets should not be held in the same physical location.

(8) Damage protection for network security of HIS: All building apertures (e.g. ventilation grilles, post boxes and drains) should be identified and critical items should be secured from vandalism.

These eight countermeasure groups involve detail countermeasures (<Table 10>). For instance, the countermeasure group "LAN Resilience" and "LAN Protection" have various detail countermeasures, which is a little different from those of hospital Y as shown in <Table 3>.

6. Conclusions and Implications

The central contribution of the study is to apply CRAMM approach to recommend countermeasures in the context of HIS. The two case studies against HIS focus on presenting the empirical procedures of the asset valuation and countermeasure recommendation. The study shows that specific computer resources and assets subject to control are categorized into several groupings. These assets are considered to have a value to the organization that uses the HIS. The main objective of asset valuation is to determine relative values which provide a means of ranking computer resources with a given operating environment rather than providing an accurate estimate of asset values.

Because everyday life in many ways depends on the sharing of information, personal privacy must be defined within that social context. Privacy is the degree of control that individuals have over the distribution of facts about themselves, it is the right to a reasonable expectation of confidentiality. Patient records are the primary repositories of data in the information-intensive health care industry. Health care professionals today face an unprecedented information explosion as the quantity and complexity of patient data and medical knowledge increase daily. Uniform national standards of HIS network security should be developed for patient records maintained by health care institutions. Fair information practices and the provisions of the Privacy act form the bases for most initiatives to protect medical information. This study suggested countermeasures for minimization of risks of computerized medical information, using CRAMM, which is possible through input of CRAMM questionnaire and interview. Network security management were described for the HIS and the results will help improve the security management of HIS network and computerized medical information.

The objective of recommendation of HIS controls is reasonable assurance as opposed to absolute assurance. The threats to computer resources are made to be minimized rather than eliminated from the implementation of the controls. It is impossible to eliminate all risks, no matter how many security and controls are established in IS.

The result of this study should serve as a baseline to stimulate additional studies in this area. Full risk management are necessary to analyze for integrated HIS. However, in order to fully analyze security of HIS more completely, a

number of hospital and specific technical alternatives of HIS network security management should be investigated. Further, it is necessary to obtain responses from a number of interviewees and a diverse source of inputs (e.g., various documentation, public information) for the correctness of risk management. If the response to CRAMM questionnaire is faithfully made though various sources, the recommended countermeasures would be more reliable and complete. In addition, it is need to develop more technical security method for guards of medical information in balance with various procedural countermeasures suggested through CRAMM to cope with the sophistication of HIS as the integration and utilization of HIS proceed. Next, this study did not undertake any explicit threat and risk analysis because of difficulty in identifying threats and probabilities of their occurrence. The impact analysis of the threats in terms of unavailability, destruction, disclosure, and modification are performed instead in Case Y. The risk analysis need to be performed quantitatively to enable more subtle recommendation of controls for HIS. Furthermore, the valuation of assets and recommendation of countermeasures are limited to physical assets and their controls. Other assets and controls should be considered in future study. Lastly, the database of the CRAMM countermeasures should be updated when the environments (e.g., size, organizational structure, system update) of hospitals change.

References

[1] Bakker, A.R. "Security in medical informatics systems," In yearbook of Medical Informatics, 1993, pp.52-60.

[2] CCTA, *CRAMM User Guide*, Central Computer and Telecommunications Agency, 1993.

[3] Cooper, J.A., *Computer and Communication Security*, McGraw-Hill, 1989

[4] Czecowski, J.A. and Bruce, R.R.A, "Privacy and Confidentiality of Health Care Information," American Hospital Publishing, Inc., 1988.

[5] Dennison, M.W.L. and Toth, K.C., "Practical Models for Threat/Risk Analysis," Proceedings of the 14th National Computer Security Conference, 1991, pp.427-435.

[6] Dick, R.S. and Steen, E.B., "The Computer-Based Patient Record," National Academy Press, 1991.

[7] Duyn, V.J., *Personnel Security Policy Critical to Dispel Risk*, UMI Company, 1995

[8] Elbra, R.A., "Computer Security Handbook," NCC Blackwell Limited, 1992.

[9] Ford, W., "Computer Communications Security," Prentice-Hall Inc., 1992.

[10] Jung, B., "A Study on Risk Analysis and Security Mechanisms for the Internet Security," Master Thesis, Korea Advanced Institute of Science and Technology, 1995.

[11] Kim, D., *Activate Information Using of Medical Department*, Institute of Health Society, 1995.

[12] Loch, K.D., Carr, H.H., and Warkentin, M.E., "Threats to Information Systems: Todays Reality, Yesterdays Understanding," *MIS Quarterly*, June (1992), pp.173-186.

[13] Louwerse, C. P., Kouwenberg, J.M.L., *Data Protection Aspects in an Integrated HIS*, UMI Company, 1995

[14] MEDINFO 95 Eighth World Congression

Medical Informatics Vancouver, British Columbia Canada, July, 1995, pp.23-27.

[15] Merriam-Webster, *Websters Ninth New Collegiate Dictionary*, G & C. Merriam Company, Springfield, MA, 1989.

[16] Muftic, S., *Security Mechanisms for Computer Networks*, John Wiley and Sons, 1989.

[17] National Research Council (NRC), *Computers at Risk: Safe Guarding in the Information Age*, System Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Academy press, 1991.

[18] Office of Technology Assessment (OTA), *Protecting privacy in Computerized Medical Information*, U.S. Congress, Washington, DC: U. S. Government Printing Office, September, 1993.

[19] Parker, D.B., *Computer Security Management*, Reston 1981.

[20] Pernul, G., "Information Systems Security: Scope," State-of-the-Art, and Evaluation of Techniques, *International Journal of Information Management*, Vol.15, No.3 (1995), pp.165-180.

[21] Pfleeger, C.P., *Security in Computing*, Prentice Hall, 1989.

[22] Pierson, L.G. and Witzke, E.L., "A Security Methodology for Computer Networks," *AT&T Technical Journal*, May/June, 1988.

[23] Rainer, R.K. Jr., Snyder, C.A., Carr, H.H., "Risk Analysis for Information Technology," Journal of Management Information Systems, Vol.1, No.1, Summer (1991), pp. 129-147.

[24] Shin, K., "A Study about Construction Currency of HIS and Development Direction," Working Paper, Korea Uuiversity, 1993.

[25] Smith, M.R., "Computer Security - Threats, Vulnerabilities and Countermeasures," *Information Age*, Vol.11, No.4, October (1989), pp.205-210.

[26] Stallings, W., *Data and Computer Communications*, Fourth Edition, Macmillan, 1995.

[27] Straub, D.W.Jr., "Effective IS Security: An Empirical Study, Information Systems Research," Vol.1, No.3, 1990, pp.255-276.

[28] System Security Study Committee (SSSC), *Computers at Risk*, National Academy press, 1991.

[29] TANG, A. and Scoggins, S., *Open Networking with OSI*, Prentice-Hall Inc.,1992.

[30] Tompkins, F.G., "How to Select a Risk Analysis Software Package," *DATAPRO Classic on Information Security Service, Risk Management*, December (1995a), pp. 1-5.

[31] Tompkins, F.G., "Information Security Risk Management," *DATAPRO Classic on Information Security Service, Risk Management*, December (1995b), pp.1-18.