Risk Analysis and Security Management of IT Information in Hospital

Suratose Tritilanunt and Autthapon Tongsrisomboon
Department of Computer Engineering, Faculty of Engineering, Mahidol University
25/25 Phuttamonthon sai 4, Salaya, Phuttamonthon
Nakhon Pathom, Thailand 73170

***Abstract*— This paper proposes a technique to apply the risk assessment framework into the information system of the hospital in Thailand. By using our proposed framework, the hospital's IT administrators would be able to manually collect and evaluate some system vulnerabilities and risk of the IT system by themselves. The risk assessment framework consists of 6 steps including (1) Information gathering, (2) current capabilities to control vulnerability, (3) Number of threat occurrence from the past, (4) Evaluation of threat's likelihood, (5) Threat's impact measurement, and (6) Risk evaluation and determination. This research applies the technique called Vulnerability Assessment and Penetration Testing in order to explore system vulnerabilities inside the IT system, and subsequently examine the capability to control these vulnerabilities. After developing a conceptual model and process of risk assessment, this framework has been used at 2 medium-size hospital. As the pre-forecasting evaluated from factors such as system readiness, hardware readiness, user readiness, as well as the proposed technique in which develop check list and check sheet to examine the sysytem, the results are consistent with the outcome when we apply our conceptual framework into the hospital's IT system. Moreover, the experimental result shows the risk inside the IT system, severity of vulnerability and consequent impact that may occur when IT system is under attack. The results of this research can be used to fix and strengthen the IT system in the hospitals in order to efficiently reduce the level of risks.**

***Index Terms*— Risk Analysis; Risk Assessment; Information Security; IT Security System of hospital; IT Security Standard; HIPAA; ISO 27001; Penetration testing**

I. INTRODUCTION

Large- and medium-sized hospitals in Thailand currently employ information technology in health care, communication, data storage and retrieval, disease analysis, therapy, finance, etc., all aimed at improving patient care efficiency. Data storage and retrieval play significant roles in the patient's diagnosis, e.g. Electronic Health Record (EHR) or Electronic Patient Record (EPR), etc. Hospital information technology systems are clearly beneficial for service provision to patients. There are, however, disadvantages because internal and external communications can be attacked by hackers, e.g. by taking over the system and revising or copying data as well as making the existing servicing system fail to the point that service provision is no longer possible, which will result in severe impacts on hospitals in terms of reputation and patient confidence, and even patient safety in some cases. Thus, data security systems are vital in protecting the IT data in hospitals from potential attacks. However, many of them try to invest in security devices such as firewall and antivirus. They do not realize to implement in intangible way such as risk analysis [1].

In order to know that the information system we are using is sufficiently safe and secure, risk assessment is of tremendous importance. Risk is the negative impact of the exercise of vulnerability. Risk analysis is the process of identifying risk, and considering planning to reduce risk to an acceptable level. The proposed framework is adapted from the general concepts presented in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 [2].

The main objective of this research is to develop evaluation process for risk analysis by using a document checklist and check sheet, as well as a penetration testing technique [3, 4, and 5] which suit for evaluating IT security system for health-care organization in Thailand. This research referred to two IT security standards, health insurance portability and accountability (HIPAA) and ISO27001, in order to create checklist for analyzing system's vulnerability and current control. This is because HIPAA is the IT security standard of health information and ISO is the global standard which cover all section of IT security system. To understand the difference of HIPAA and ISO 27001, Sheldon Borkin studied the comparison of HIPAA Final Security Standards and ISO27001. The different of these two standard are HIPAA mainly focuses on electronic personal health information (ePHI) but ISO27001 is worldwide IT security standard and cover mostly section of IT security domain [6].

Manuscript received November 12th, 2013. This research is supported by the Office of the Higher Education Commission and Mahidol University under the National Research Universities Initiative.

S. Tritilanunt is with the Department of Computer Engineering, Faculty of Engineering, Mahidol University, Thailand (e-mail: suratose.tri@mahidol.ac.th).

A. Tongsrisomboon is with the Department of Information Technology, Faculty of Engineering, Mahidol University, Thailand (e-mail: suratose.tri@mahidol.ac.th).

II. Risk Analysis Process

In this paper, we propose a conceptual framework to analyze risks in the IT system of the hospital. In order to obtain a result used as a risk indicator, the framework consists of three essential process including; information gathering, information evaluation and matrix assessment as shown figure 1.

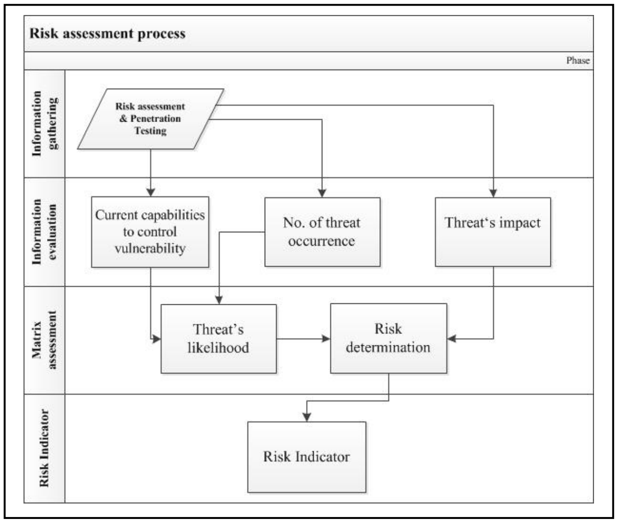


figure 1. Risk analysis process

A. *Information gathering*

This paper implements risk assessment and penetration testing in hospital data collection, which will have more effective and accurate outcomes than data collection from questionnaires used in previous data collection procedures in the risk analysis process [7]. This is because data collection from questionnaires may be subject to errors from reliance on the respondents' subjective feelings. Moreover, penetration testing can reveal the vulnerability in information systems and potential impacts on a hospital.

Information gathering of information system from the hospital comprises of 3 processes;

1) Network Vulnerability Scanning: Vulnerability scanning is importance procedures that can be used to indicate the vulnerability on the target, the severity level, and the impact to the system. In order to be able to find the solution, a famous tool known as Nessus is an example tool used to assist in the vulnerability identification. The result of vulnerability scanning tool would be a vulnerability severity scoring criteria from CVSS.

2) Database and Web server Vulnerability Scanning: Database and web server vulnerability assessment is a process for locating a server's vulnerabilities, i.e. providing web server and database services by using tools and command sets to test for the vulnerabilities. Some example well-known vulnerabilities in the web server are attack in the form of XSS (Cross site scripting) and SQL injection.

3) Exploitation: Exploitation is the step for testing the system attack using the data acquired from previous steps to find out what extent of impacts the vulnerability located has caused and how to access the vulnerability. In this study, a program, Metasploit, was used to test the system attack. Metasploit is a program used to develop an attack in the form of exploitation, which is an attack using vulnerabilities so the user gains access, control or any actions on the target computer. Hence, Metasploit is a program that can be used to test the vulnerabilities of a computer and network system in order to find ways to protect and fix the problem against the vulnerabilities. The test attack has two forms, namely, testing on an actual system and testing on a simulated system.

TABLE I. Mapping actual system and simulated system

Mapping	Actual system	Simulated system
1) Place	Live place	Lab room
2) Accuracy	Accurate	Less than Actual system
3) Impact	Yes. It may cause some damages to a system and information	No, because Simulated system takes information to test in lab room that is not have impact on live system

B. *Information evaluation*

This step involves the analysis of data acquired from the first step. This step is divided into three the following three sub-steps:

1) Current capacity to control vulnerability: This is the step for identifying vulnerabilities and the ability to control vulnerabilities. We use an instrument to test the vulnerabilities which allows us to know the number of all existing vulnerabilities and their severity in order to identify the ability to control the vulnerabilities. From [8, 9, and 10], there are 13 types of threat's source, which reviewed from general threat of IT system.

Control analysis is a procedure in capability to control vulnerability assessment. This step uses the value from Vulnerability Identification procedure to compare with the Table II. The number of vulnerability and severe level of that vulnerability can tell the current capability to control vulnerability. Table II presents the relationship between capability to control vulnerability and severity level of vulnerability. And vulnerability severity can be obtained from processing the Nessus program by using vulnerability severity scoring criteria from CVSS.

TABLE II. Current Capabilities to control

Capability to control vulnerability	**Severity of vulnerability**	**Description**
Low	Critical	The most of examine vulnerability are critical show that the capabilities to control vulnerability are low
Medium	High	The most of examine vulnerability are high show that the capabilities to control vulnerability are medium
High	Medium	The most of examine vulnerability are medium show that the capabilities to control vulnerability are high
Excellent	Low	The most of examine vulnerability are low show that the capabilities to control vulnerability are excellent

2) Number of threat occurrences: This procedure is used for analyzing the information that get from Number of threat occurrence information. Table III presents the value of Number of threat occurrence, which separated into 4 groups as follows, 1) 1-25 times 2) 26-50 times 3) 51-75 times and 4) 76-100 times.

TABLE III. Number of threat occurrence

Threat-Source	**Number of occurrence**			
IT Threat	1-25	26-50	51-75	76-100
Hacker				

3) Threat's impact: This procedure is evaluation of data from pierce system test by use all threats occurrence to combine with type of attacks that is Fabrication, Modification, Interruption, and Interception that use to compare with value in Table IV to find the impact level from threat occurrence by unexpected person divided into 4 levels that is Severe, Serious, Significant, and Minor to use in the risk determination in next procedure.

TABLE IV. Relationship between Threat's impact and Attack

Impact	**Type of attack**	**Description**
Severe	Fabrication	a person or program that not allow to counterfeit information in server
Serious	Modification	a person or program which it not allow access to resource and modify data
Significant	Interruption	damaged of resources that make service stop working or cannot access to server again
Minor	Interception	a person, program, or computer not allow to access to the resource or information

- Fabrication causes severe impacts to the system because the attacker can falsify or generate data not existing in the hospital's system, e.g. by sending a set of commands for creating user accounts not existing in the system to run the program desired by the attacker or to open a vulnerability so the attacker gain control of the target machine, enabling the attacker to gain control over the target. Therefore, if an attacker attacks the hospital system by gaining control of the entire server, the attacker may steal key data, falsify data and eventually cause the hospital's IT system to stop service provision. Thus, the severity is at severe level.

- Modification affects the system to a serious degree because the attacker can access the hospital's resources or amend internal data. The attacker may amend the hospital data as well as medical records which can result in erroneous patient treatment. Thus, the severity is at a serious level.

- Interruption causes significant impacts because the attacker can destroy system resources causing the system to fail or no longer function, which causes impact on the hospital's services such as patient services, data searching and medicine dispensing. If the server stops functioning, it can be remedied by rebooting. Thus, the severity is at significant level.

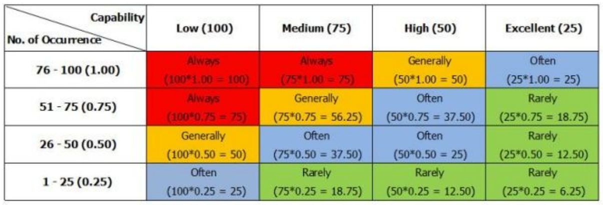
- Interception causes impacts to a minor degree because the attacker gains access to resources or data. In this case it is the intercepted data but it does not affect the hospital's IT system in any way. Thus, the severity is at a significant level.

C. *Matrix assessment*

1) Threat's likelihood: This step is the matching of values from the steps on Current Capabilities to Control Vulnerability and Number of Threat Occurrences in the 4 x 4 matrix table (Table V) to find the chance or possibility for an attack to occur. It is divided into the following four levels: rarely, sometimes, often and always.

According to Table V, the values of current capacity for controlling vulnerability are set at: Excellent = 25, High = 50, Medium = 75 and Low = 100, and the number of threat occurrences are set at 1 to 25 = 0.25, 26 to 50 = 0.50, 51 to 75 = 0.75 and 76 to 100 = 1.00.

TABLE V. The 4x4 Likelihood Matrix [7]



Capability / No. of Occurrence	Low (100)	Medium (75)	High (50)	Excellent (25)
76 - 100 (1.00)	Always (100*1.00 = 100)	Always (75*1.00 = 75)	Generally (50*1.00 = 50)	Often (25*1.00 = 25)
51 - 75 (0.75)	Always (100*0.75 = 75)	Generally (75*0.75 = 56.25)	Often (50*0.75 = 37.50)	Rarely (25*0.75 = 18.75)
26 - 50 (0.50)	Generally (100*0.50 = 50)	Often (75*0.50 = 37.50)	Often (50*0.50 = 25)	Rarely (25*0.50 = 12.50)
1 - 25 (0.25)	Often (100*0.25 = 25)	Rarely (75*0.25 = 18.75)	Rarely (50*0.25 = 12.50)	Rarely (25*0.25 = 6.25)

Likelihood Scale: Rarely (0.00 - 24.99), Sometimes (25.00 - 49.99), often (50.00 - 74.99), Always (75.00 - 100.00)

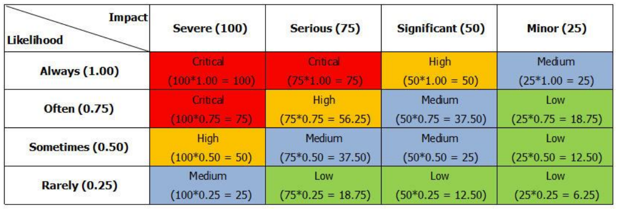
*capability of current control to control vulnerability

2) Risk determination: This is the step of comparison between Threat's likelihood and Threat's impact procedure that uses a 4x4 matrix table (Table VI) to identify the hospital technical risk. It is divided into four levels, namely, low, medium, high, and critical.

According to Table VI, the value of a threat's likelihood are set a Rarely = 0.25, Sometimes = 0.50, Often = 0.75 and Always = 1.00, and the threat's impact values are set at Minor = 25, Significant = 50, Serious = 75 and Severe = 1.00.

3) Risk Indicator: This step involves the summary of all results acquired from the aforementioned processes. The results are divided into four levels, namely, 1) Critical, 2) High, 3) Medium and 4) Low.

TABLE VI. The 4x4 risk level matrix table



Impact / Likelihood	Severe (100)	Serious (75)	Significant (50)	Minor (25)
Always (1.00)	Critical (100*1.00 = 100)	Critical (75*1.00 = 75)	High (50*1.00 = 50)	Medium (25*1.00 = 25)
Often (0.75)	Critical (100*0.75 = 75)	High (75*0.75 = 56.25)	Medium (50*0.75 = 37.50)	Low (25*0.75 = 18.75)
Sometimes (0.50)	High (100*0.50 = 50)	Medium (75*0.50 = 37.50)	Medium (50*0.50 = 25)	Low (25*0.50 = 12.50)
Rarely (0.25)	Medium (100*0.25 = 25)	Low (75*0.25 = 18.75)	Low (50*0.25 = 12.50)	Low (25*0.25 = 6.25)

Risk Scale: Low (0.00 - 24.99), Medium (25.00 - 49.99), High (50.00 - 74.99), Critical (75.00 - 100.00)

The outcome of the risk indicator tells us about the likelihood or possibility for the threat to successfully attack the hospital's IT system. The results are from Table VI. For example, if the likelihood is often, the threat success is indicated to range from 0.51 to 0.75 and impact on the IT system is at a significant level, thereby causing the risk assessment to be within a medium range, i.e. the risk occurring with the hospital's information system is moderate.

III. EXPERIMENTAL RESULTS

This paper gathered the data from two hospitals, so called hospital A and hospital B. Both hospitals are categorized as a medium-size hospital. The experimental result is then compared with the hospital A, which was examined using check list and check sheet technique proposed by [7]. In that paper, they use the check list evaluation in order to evaluate the security readiness of the information system used in the hospital. Following are short summarized of the process and calculation in order to create a risk indicator of IT system in the hospital.

The results of this paper are presented into two perspective relate to two methods of analyzing risk, which are checklist evaluation compared to and penetration testing evaluation (hospital A). At the end, we extend our proposed model to another hospital, so called hospital B, in order to test the functionality and effectiveness of the risk analysis framework.

A. Checklist evaluation method's result and Penetration testing method's result for Hospital A

In this research we used On-site Interviews method as information gathering techniques. Interviews with IT system support and management personnel can enable risk assessment personnel to collect useful information about the IT system (e.g., how the system is operated and managed). On-site visits also allow risk assessment personnel to observe and gather information about the physical, environmental, and operational security of the IT system.

The main factors to determine risk level is likelihood and impact of threats. So table VII shows the possibility of likelihood of each method from hospital A.

TABLE VII. The results of likelihood determination of hospital A

Method	**Checklist [7]**	**Penetration testing**
Threat-Source	**Hospital A**	**Hospital A**
IT Threats		
External Threats		
Hackers	Rarely	Rarely

Table VII compares the threats, the likelihood of method. The results of hacker threat show no difference for the likelihood level.

The main second factor to determine threat level is the impact of each method. Table VIII shows the impact assessment from hospital A.

The Table VIII, The result of hacker threat show that Penetration testing method's impact level is higher than Checklist method.

TABLE VIII. The impact assessment of hospital A

Method	**Checklist [7]**	**Penetration testing**
Threat-Source	**Hospital A**	**Hospital A**
IT Threats		
External Threats		
Hackers	Minor	Severe

To measure risk, a risk scale and a risk-level matrix must be developed as Table VI. The results of this step are presented in four levels of risk for each threat; Critical, High, Medium, and Low. Table IX presents the results of risk analysis for both methods.

TABLE IX. Risk indicator of hospital A and hospital B

Method	**Checklist [7]**	**Penetration testing**
Threat-Source	**Hospital A**	**Hospital A**
IT Threats		
External Threats		
Hackers	Low	Medium

Table IX is showed that Checklist evaluation method's risk indicator has less risk level. And Penetration testing method's risk indicator has more risk level, which in medium level. Because Checklist evaluation method used interviewing technique for gathering information about complying with HIPAA and ISO27001 standards , threats no of occurrence, threat's impact, and priority weight of information system domain. The interviewees are the system administrator and IT manager from hospital, so the answer may come out with interviewee's private opinion or bias to the organization, which can make the result change more or less. Some interviewee may not want their organization look unsecure, so the answers may be too optimistic or they may negligence to some problem. Another may be upset with their inappropriate responsibility, so the answer may be too pessimistic or they were unhappy with their work. Beside that there was some interviewees answer the question injudicious or act like they know the answer for sure.

But Penetration testing method implements risk assessment and penetration testing in hospital data collection, which will have more effective and accurate outcomes than data collection from questionnaires used in previous data collection procedures in the risk analysis process [7] and penetration testing can reveal the vulnerability in information systems and potential impacts on a hospital.

From a success of the testing result of Hospital A using a proposed conceptual framework for risk assessment, we extend our experiment to another medium-sized hospital, so called Hospital B. The experimental result will be presented in the next section.

B. Penetration testing method's result for Hospital B

1) Hospital B: In this case study, the researcher collect additional data for database and web server because currently there are more attacks in the forms of XSS (Cross site scripting) and SQL injection, which are very harmful vulnerabilities because attackers can steal the user's data and can pass through the system's identity verification.

Hospital B is also a medium-size hospital like Hospital A, but with more servers than Hospital A by 12. Fourteen servers are for patient services and two are for web server.

The test objectives are to assess the risk of the operating system that is functioning on the hospital's servers. The IT system test scope is database vulnerabilities scanning, web server vulnerabilities scanning, and penetration testing and risk assessment.

After the vulnerability scanning in this case study, it was revealed that a total of 125 vulnerabilities existed in the hospital's 18 servers, with 50% occurring to OS that are Windows servers 2003, 26% occurring with Windows server 2008 and 24% are Windows server 2008 R2. The attacks can be categorized, as shown in figure 2, into the following 10 formats: 1) Code execution; 2) Authentication-bypass; 3) SQL Injection; 4) Elevation of Privilege; 5) Brute-force; 6) Buffer overflow; 7) Denial of service; 8) Information gathering; 9) Man in the middle and 10) Cross-site scripting, as shown in Figure 3 and Table X. Most vulnerability is medium level.

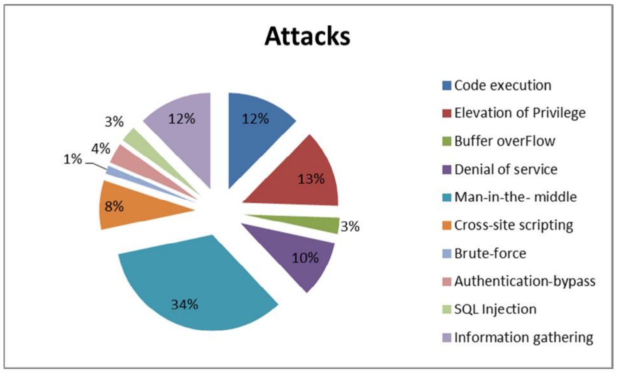


Figure 2 Attacking technique at Hospital B.

- *Man in the middle* is when a person maliciously asserts him/herself in the middle of a conversation between two people and acts as a medium for the receiving/sending of data by the two parties in the conversation and the person maliciously uses this kind of attack to intercept or alter data communicated by the two parties.
- *Cross site scripting* is when a script or code embedded in the target's web browser to intercept key data of the target or set up a link to the site as prepared by the malicious party.
- *Brute force* involves password decoding using various programs to gain access to the system.
- *Authentication bypass* means passing the system's vulnerability without having to go through identity verification.
- *SQL injection* is an attack by the SQL string in the system so it displays the data sought by the malicious party.
- *Information gathering* is the collecting of the target's necessary data for subsequent use in the attack.

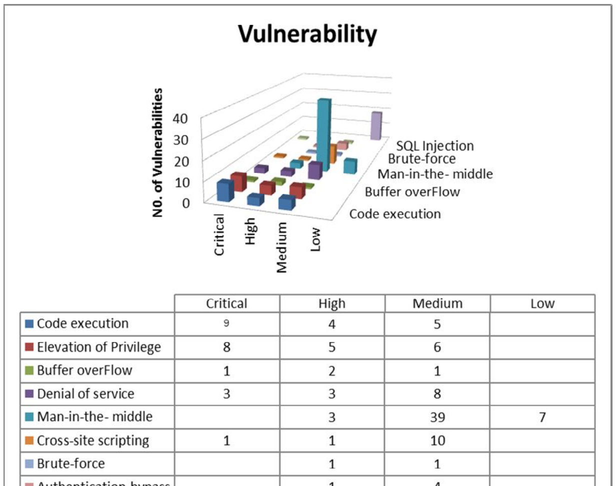
a) Current capabilities to control vulnerability: Vulnerability assessment discloses that most vulnerability is at high level. When comparison is made in Table II, it can be concluded that current capabilities to control vulnerability are at ***"High"*** level because most vulnerabilities are at a high level.

b) Number of threat occurrence: Because the number of threat occurrences to the hospital is twice, the number of threat occurrences falls within a range of 1-25 times, which is the lowest level.

c) Threat's impact: Once the attackers' attack characteristics are known, the type of attack can be identified as shown in Table X and the type of impact occurring to the IT system will also be identified as compared in Table IV. The level of impact occurring to this hospital is "***Minor***".

d) Threat's likelihood: This is the step for comparing the current ability to control the vulnerability with the number of attacks occurring during the previous two years in Table V. In this case study: The capability level of current vulnerability controlling: Medium and The number of threat occurred in past 2 years: 0-25.Therefore the opportunity or likelihood of threat occurrence from hacker is in level: ***"Rarely".***

e) Risk determination: This is the step for comparing the possibility for the attack to occur with the potential level of impact on the hospital's IT system in Table VI. In this study: The opportunity or likelihood in threat occurrence from hacker: Rarely and the impact level occurs with hospital's information technology system: Minor. Therefore the risk determination of this hospital is ***"Low"*** level.



	Critical	High	Medium	Low
■ Code execution	9	4	5	
■ Elevation of Privilege	8	5	6	
■ Buffer overFlow	1	2	1	
■ Denial of service	3	3	8	
■ Man-in-the- middle		3	39	7
■ Cross-site scripting	1	1	10	
■ Brute-force		1	1	
■ Authentication-bypass		1	4	

Figure 3 The number of vulnerability at Hospital B.

f) Risk indicator: This step summarizes the results acquired from risk determination. For this case study, the result revealed the risk to be ***"Low"***, thereby meaning the chance for an attack by the hacker is low. And when an attack does occur, the impact severity to the hospital's IT system will be at a low level. The system supervisor must set policy for determining whether or not plans for dealing with this kind of threat are necessary, or if the risk is acceptable.

TABLE X. Relationship between type of attack and method of attack in Hospital B

Type of attack	**Method of attack**	**Description**	**No. of Vulnerabilitie**
Fabrication	Code execution	To create and send a batch file that does not exist in the system into the system in order to control the system.	18
	Authentication-bypass	Be attack through confirmed identity of system	5
	SQL Injection	SQL Query String attack in showing needs information	4
	Cross-site scripting	Bury script in web browser for intercept target's information	12
Modification	Elevation of Privilege	Edit their information in order to obtain equivalent administrator rights.	19
	Brute-force	decrypt password for access to system	2
Interruption	Buffer overflow	Server/Service can be stopped.	4
	Denial of service	Server/Service can be stopped.	14
Interception	Man-in-the- middle	eavesdrop or intercept information the conversation of sender and receiver	49
	Information gathering	Gather the required system information.	18

2) Guideline for Reducing the Risks of the Hospital's IT System: According to data collection, the hospital is exposed to low level of risk. Thus, whether the correction is necessary or not it depends on the system supervisor who can perform the following:

a) Risk Management Guideline at the Server Level: The testing can reveal that the hospital's system still has vulnerabilities occurring on the software installed on the server. Thus, this software should be updated to minimize the number of vulnerabilities. This step is a method for minimizing risks that requires a low budget and time to manage the risk. In addition, the server can be installed with an anti-virus program, a firewall and HIDS/HIPS using a complex password, unnecessary users can be deleted from the system, file permission settings should be more strict, alien programs should be checked consistently so there is no remote use of protocol without being coded (for example telnet or ftp), limit IP address and user account of people who remotely use the server.

b) Risk Management Guideline at the Network Level: This level involves the protection of vulnerabilities remaining in the system by installing additional security devices in the system such as protecting MITM using switch that allows the setting of MAC Filter and IP filter on each port or by using Static ARP. Authentication should be required to verify user name and password before permission is granted to connect to the internet. There should also be protection against Rough DHCP and IP address falsification. MAC addresses should be installed with patches, an antivirus program and a personal firewall to protect the client's machine and caution should be exercised concerning folder sharing settings.

c) Risk Management Guidelines with Technological Modifications: According to the testing, one server runs Windows server 2003. A strategic planning by changing technology can be set up, namely, the OS in this case. Considerations must be given in multiple aspects such as whether or not former application programs are compatible with the new OS.

IV. DISCUSSION

From the result, it can help organization invests more precisely with the IT security system by reference from risk level prioritization. There are necessary actions to manage risks or to plan the IT security strategies as Table XI.

TABLE XI. Risk scale and necessary actions

Risk Level	**Risk Description and Necessary Actions**
Critical	If an observation or finding is evaluated as a critical risk, there is a extremely strong need for corrective measures. An existing system may no longer to operate, so a corrective action plan must be put in place immediately.
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these

	actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's administrator must determine whether corrective actions are still required or decide to accept the risk.

Hospital A is at medium risk. Thus, there should be planning to minimize risks at suitable times or when there is a chance to do so.

Hospital B is at low risk. Thus, the system supervisor needs to decide whether or not the existing risks are acceptable and whether or not additional vulnerabilities need to be identified/detected and examined.

A. *Number of threat occurrence*

The risk assessment of both hospitals revealed the risk existing in the hospital, i.e. Hospital A is at moderate risk and Hospital B is at low risk. It is evident that both hospitals are exposed to mildly severe risks because the factor affecting risk intensity is the number of threat occurrences and neither hospital has ever been attacked or known that they had ever been attacked. Thus, the number of occurrences in these cases falls within a range of 1-25 times resulting in a rating of rarely for threat's likelihood. When mapping with threat's impact, which is severe (Hospital A) or Minor (Hospital B), the results remain at moderate or low risk levels.

Initial data collection reveals that both hospitals lack records on attacks by hackers, possibly because the hospitals give greater importance to patient services than security and neither hospital has ever had any severe impacts on their IT systems, causing them to pay less attention to this aspect. Thus, data collection for concerning this aspect is done in the manner of interview forms and data received may deviate from reality because the answers are dependent on the respondents' feelings.

B. *Server Vulnerabilities*

Another factor affecting risk intensity is the IT system's vulnerabilities, which are the weak points of the IT system. The number and severity of vulnerabilities reveal current capabilities to control vulnerability, method of attack and threat's impact occurring to the IT system. Capabilities to control vulnerability and impact to the IT system are correlated with the hospital's IT risk intensity.

According to Table XII, both of the hospitals in this case study are medium-size hospitals, but the IT system sizes are clearly different. Hospital A has only six servers, which is smaller in number than Hospital B by 12 servers. However, due to differences in IT system management, Hospital B with its higher number of servers clearly has a lower number of vulnerabilities than Hospital A. As a result, Hospital B's current capability to control vulnerability is at a high level and threat's impact is at a minor level. Thus, the risk assessment results are that Hospital B is exposed to lower risk than Hospital A, which has a medium level of risk.

TABLE XII. Mapping result of Hospital A and B table

Hospital Results	Hospital A	Hospital B
Vulnerability	High	Medium
Current capabilities to control vulnerability	Medium	High
Number of threat occurrence	1-25	1-25
Threat's likelihood	Rarely	Rarely
Impact	Severe	Minor
Risk	Medium	Low

C. *Testing Environment*

Because hospitals are places with extremely sensitive data and because it would be very risky for a hospital to stop functioning or for a hospital's data to be damaged during the testing, penetration testing could not be applied to the hospital's IT system at the actual location because the process could have caused severe damage to the hospital's IT system and might have caused the system to stop functioning. Thus, a server had to be simulated for the process of penetration testing.

There is a disadvantage to server simulation in that 100% of the server cannot be simulated because the values cannot be set or configured in the same way as the system supervisor. This may cause the results from penetration testing to deviate from reality. Thus, a server cloning method should be used rather than the server simulation method because server cloning can imitate 100% of the server and the results following penetration testing are accurate and precise. However, because neither of the hospitals in this study approve of server cloning, the data acquired from penetration testing may contain errors.

D. *Security awareness*

This is the step overlooked by many people. In practice, however, it is a "must-do" and needs to be done on an annual basis. Training should be held so the staffs in the organization gain correct understanding on the issue of computer data security. The training should begin from high-ranking executive and middle management levels which should be followed by a system supervisor and those who are directly responsible for information security, internal audit and general computer users to prevent them from becoming victims of viruses or programs infiltrating to destroy systems that usually come with email attachments and visits to inappropriate websites.

According to the case study, Hospital A's IT system has been developed continually by the IT and outsourcing departments. However, because it is focused on IT development for patient data management and because the hospital has never been attacked by hackers, the hospital lacks awareness and readiness to prevent itself from hackers. For example, The hospital never updates patches/hotfixes, thereby causing the vulnerability test in the hospital's IT system to reveal that Hospital A has numerous vulnerabilities at a severe level that may become channels for hackers to attack and steal data from the hospital. Moreover, according to the case study, Hospital B has a larger IT system than Hospital A, but because Hospital B's IT system has developed continually and the hospital has clear policy enabling Hospital B to improve its IT system together with maintaining patient data security. In addition, the hospital's IT department has knowledge and understanding about IT security. For example, Hospital B maintains and updates its patches/hotfix regularly and consequently had less vulnerability detected than Hospital A.

E. Patch/Hotfix

In installing patches/hotfix, proper managerial methods should be used because patch/hotfix that may affect the system cannot be installed, e.g. applications functioning on the server may not work because the patch/hotfix installed may block the port for function the application is using, thereby causing the application to fail after the patch/hotfix installation. Thus, it is necessary to try to understand the installation of the patch/hotfix and how it may affect the system. Otherwise, a server/system may be simulated to test and determine whether or not the patches/hotfix to be installed affect the applications on the system.

V. Conclusion and Recommendations

Today, hospitals in Thailand have implemented IT systems to play significant roles in health services such as data storage, analysis, as well as conducting transactions to provide more efficient health services. There are, however, disadvantages to IT systems such as harm by natural disasters or hackers. This research focuses on threats made by hackers because the damages occurring can be severe and hospitals in Thailand still give them very little importance.

The hacker's aim is the key data of patients and hospital staff such as patient history, identification numbers, and transaction history. Thus, adopting a security system is essential for prevention against threats by hackers. In this research a risk assessment method was employed as a guideline for assessing the hospital's IT security system to determine the level of risk. Therefore, the hospital can operate with efficiency and safety. The research procedures are divided into the following four steps: Collecting essential data for risk analysis - This step begins with the study of guidelines and methods from risk assessment to data collection. In this research, the penetration testing method was used in data collection to find vulnerabilities existing in the hospital's IT system so data can be acquired for use in the next level of risk assessment. The step of information evaluation gathers data from the data collection process and analyzes it to identify the hospital's current capability to control vulnerability, number of threat occurrences and threat impact which have been obtained from the categorization of technical data on the attack to find the level of impacts on the hospital. The next step is to map the data from information evaluation step to find the level of risk by mapping current capabilities to control vulnerability to the number of threat occurrences to obtain threat's likelihood and by mapping threat's likelihood with threat's impact to obtain the level of risk of the hospital's IT system. The last step is to summarize the results from the risk assessment to identify the level of risk for threats and the risk management guidelines.

A. Information gathering

Preliminary information gathering remains inaccurate because the log file of the number of attacks cannot be acquired because the hospitals have no policy for storing the history of such information. Thus, one of the tasks of this research was to determine the number of attacks from the interviews. However, the data obtained contains a high level of errors because it is too heavily reliant on the respondents' subjective feelings. Future work, therefore, should involve data collection on an accurate number of attacks from the log files or maintenance logs of the IT system.

B. Threats

This research investigated the risk assessment of threats by hackers. In reality, threats do not come only from hackers. Natural disasters such as floods, power outages or fires can also cause damage to IT systems. Thus, both threats from hackers and other sources should be assessed in order to reveal the risks from all potential threats occurring with the hospitals' IT systems.

Acknowledgement

This research is supported by the Office of the Higher Education Commission and Mahidol University under the National Research Universities Initiative.

References

[1] E. Cavalli, A. Mattasoglio, F. Pinciroli and P. Spaggiari, "Security concepts and practices: the case of a provincial multi-specialty hospital," International Journal of Medical Informatics, vol. 73, pp. 297-303, 2010.

[2] G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology System," National Institute of Standards and Technology, 2002: Special Publication: 800-30.

[3] B. Rathore, M. Brunner, M. Dilaj, O. Herrera, P. Brunati, R. K. Subramaniam, S. Raman, U. Chavan' "Penetration testing framework," Information Systems Security Assessment Framework, 2006.

[4] K. Scarfone, M. Souppaya, A. Cody, A. Orebaugh, "Technical Guide to Information Security Testing and Assessment," National Institute of Standards and Technology, 2008: Special Publication: 800-115.

[5] A. F. Alisherov, Y. F. Sattarova, "Methodology for Penetration Testing," International Journal of Grid and Distributed Computing, 2009.

[6] S. Borkin, "The HIPAA Final Security Standards and ISO/IEC 17799," SANS Institute, 2003: Practical Assignment for GIAC GSEC Certification Version 1.4b, Option1.

[7] Chaitasanangam P. Risk Analysis and Security Management of IT Information in Hospital. Proceeding of the 2nd National and International Graduate Study Conference; 2012 May 10-11; Bangkok, Thailand; 2012.

[8] W Michael, M. Herbert, "Principles of Information Security," Boston: Inc. Thomson.

[9] International Standard ISO/IEC 27001: Reference number IS)/IEC 27001:2005(E); 2005.

[10] BS 7799 Becomes ISO 27001. BH Consulting, 2005.

S. Tritilanunt received the B.E. degree in electrical engineering from the Mahidol university, Thailand, in 1998, and the M.Eng. degree in computer engineering from King Mongkut's University of Technology Thonburi, Thailand in 2001. Later, he received Ph.D. degrees in information technology from the Information

Security Institute (ISI), Queensland University of Technology, Australia in 2008.

He is currently working at the department of computer engineering, faculty of engineering, Mahidol university, Thailand. He is an Assistant Professor who is working in the area of cryptography, computer and network security, vulnerability and penetration testing, and digital forensics. He has attended several training programs in the topics about computer and network security, risk assessment and penetration testing, and digital forensics. Recently, he holds certificates such as CCNA(Security), Ec-council Certified Ethical Hacker (C|EH), SANS GIAC Forensic Examiner (GCFE), and SANS GIAC Penetration Tester (GPEN).

A. Tongsrisomboon received the B.E. degree in irrigation engineering and civil engineering from the Kasetsart University, Thailand, in 2005 and 2007, respectively. In 2013, he received the M.Eng. degree in Science (Technology of Information System Management) from Mahidol University, Thailand.

He is interested in the computer security area. He has done research in the field of information system security. Recently, he has published a research paper "Case study: Applying of security risk assessment process for information system in hospital" in the 2012 International Computer Science and Engineering Conference (ICSEC 2012.