Journal of Information Security, **2012, 3, 169-176**
http://dx.doi.org/10.4236/jis.2012.32020 Published Online April 2012 (http://www.SciRP.org/journal/jis)

A Tree Model for Identification of Threats as the First Stage of Risk Assessment in HIS

Ahmad Bakhtiyari Shahri[1], Zuraini Ismail[2]
[1]Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia, Johor Bahru, Malaysia
[2]Advanced Informatics School, Universiti Teknologi Malaysia, Johor Bahru, Malaysia
Email: bsahmad2@live.utm.my, zurainisma@ic.utm.my

Received January 22, 2012; revised February 24, 2012; accepted March 28, 2012

ABSTRACT

Security remains to be a critical issue in the safe operation of Information Systems (IS). Identifying the threats to IS may lead to an effective method for measuring security as the initial stage for risk management. Despite many attempts to classify threats to IS, new threats to Health Information Systems (HIS) remains a continual concern for system developers. The main aim of this paper is to present a research agenda of threats to HIS. A cohesive completeness study on the identification of possible threats on HIS was conducted. This study reveals more than 70 threats for HIS. They are classified into 30 common criteria. The abstraction was carried out using secondary data from various research databases. This work-in-progress study will proceed to the next stage of ranking the security threats for assessing risk in HIS. This classification of threats may provide some insights to both researchers and professionals, who are interested in conducting research in risk management of HIS security.

Keywords: Health Information System; Threat; Security

1. Introduction

As the European Union has acknowledged, "innovation is important in today's society, but it should not go at the expense of people's fundamental right to privacy" [1]. An effective information security program includes a combination of human and technological controls to prevent loss of data, accidental or deliberate unauthorized activity, and illegal access to data [2].

However use of information and communication technology (ICT) in healthcare has created the electronic health environment and electronic health information is the core of an electronic health system that is managed by ICTs [3]. In addition because healthcare information technology has different potential to improve the quality of care and efficiency and it can also reduce medical costs and save lives so, it is currently one of the important factors for major innovations and is used in widespread around the world [4]. Therefore, if an E-health system guarantees privacy and security of patients it will succeed [5].

In recent years number of threats in health information systems (HIS) area has increased dramatically and lack of adequate security measures has caused in numerous data breaches, leaving patients vulnerable to economic threats, mental anguish and maybe social stigma. [6]. For example, between the years of 2006 to 2007 in hospitals alone, occurred exposing of more than 1.5 million names during data breaches [7]. In addition, result of 2010 Healthcare Information and Management Systems Society Security Survey suggests that the reports of more than 110 healthcare organizations have shown the loss of sensitive Protected Health Information or Personal Identifying Information affected over 5,306,000 individuals since January 2008. They were received as theft (stolen laptops, computers, or media), loss or negligence by employees or third parties, malicious insiders, system hacks, web exposure, and virus attacks [8]. So, storage information in electronic format increases the concerns about the security and privacy of patients [9]. Another study has shown that healthcare information systems of accidental events and deliberate action threats are two parameters that can severely damage HIS reliability and have negative effects on HIS [10]. However, poor organization of security measures, lack of an integrated security assessment architecture and framework and low awareness of risk analysis practices also need particular attention. As in developed countries standards of framework use in place. For example, using ISO/IEC 27002 (ISO 27799:2008) or the Health Insurance Portability and Accountability Act (HIPAA) in the healthcare environment in protecting computerized information assets [11].

By understanding the threats to health information security, the organization can better protect its information assets and strengthen the level of protection of information in health information system. Therefore management of E-Health information needs to identify the threats for an effective framework by considering the comprehensive incorporation of confidentiality, integrity and availability to be the core principles of information security. This raises major challenges that require new exhaustively attitudes such as a wide variety of policies, ethical, psychological, information and security procedures [5,12]. Hence the objective of this paper attempt to provide an up-to-date categorize of threats to healthcare assets.

2. Review and Role of Identification of Threats in Information Security Risk Management

Risk assessment requires an understanding of the threat sources, threat action and how that sources can be exploited vulnerability in a health information asset [4]. Although identifying of threats in information system is crucial stage in risk management [13] and discussion about privacy and security [12] has long been a major subject in the social science and business press, there has been controversy about lacking a systematic investigation to identify and categorize various sources of threats of information security and privacy in academic literature [6].

Figure 1 shows a conceptual framework for implementing of information security in HIS. This figure was adopted from works of Z. Ismail, *et al.* [14] and A. Yasinsac, *et al.* [15]. It was further adapted to include inputs, output, and also process of some steps. Based on ISO/IEC27002 [16] risk assessment is a critical strategy and identification

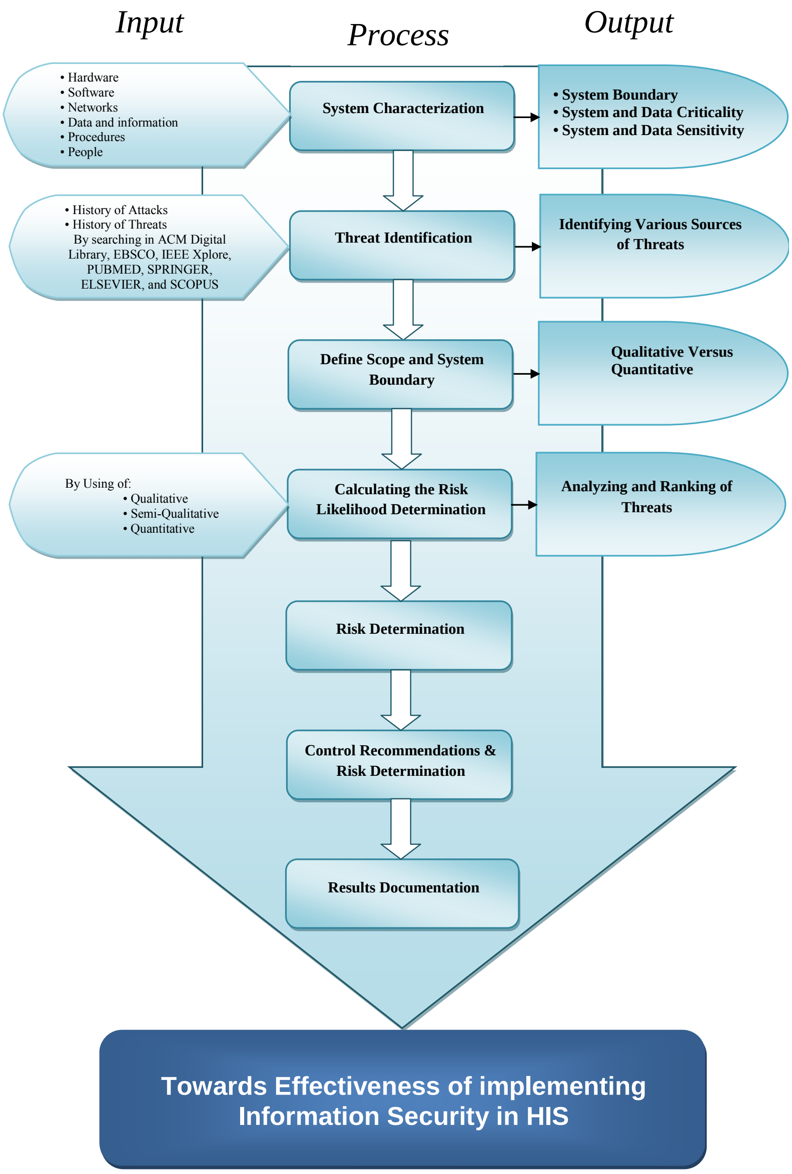

Input
Process
Output
• Hardware
• Software
• Networks
• Data and information
• Procedures
• People
System Characterization
• System Boundary
• System and Data Criticality
• System and Data Sensitivity
• History of Attacks
• History of Threats
By searching in ACM Digital Library, EBSCO, IEEE Xplore, PUBMED, SPRINGER, ELSEVIER, and SCOPUS
Threat Identification
Identifying Various Sources of Threats
Define Scope and System Boundary
Qualitative Versus Quantitative
By Using of:
• Qualitative
• Semi-Qualitative
• Quantitative
Calculating the Risk Likelihood Determination
Analyzing and Ranking of Threats
Risk Determination
Control Recommendations & Risk Determination
Results Documentation
Towards Effectiveness of implementing Information Security in HIS

Figure 1. Conceptual Framework of Information Security.

of threats is one of the important stages in every Information Security framework [17,18]. Kotz recommended that the first step of HIS framework is to identify threats to patients' identity [19]. This is because it will help in conducting risk assessment and to assist in the development of health care security policy, guidelines and laws [4,15,20]. Hence, issues of security, identification and taxonomy of threats in the field of health care organizations are important and are mandatory parameters for health information systems [11,18].

Therefore, the research question for this paper is to categories the security threats to HIS. The next section will discuss the possible security threats to HIS.

3. State of Information Security Research in Healthcare

This section presents a comprehensive review of literature of threats to HIS. The results of CSI/FBI Annual Computer Crime and Security Survey in 2002, ranked the followings as significant threats: Virus, Insider Abuse of Net Access, Laptop, Denial of Service, Unauthorized Access by Insiders, System Penetration, Theft of Proprietary Info, Financial Fraud, Telecom Fraud, Sabotage, Telecom Eavesdropping, Active Wiretap [21].

According to Ref. [22] the most important threats about patients' confidentiality are: Accidental Disclosures, Insider Curiosity for infringers own curiosity or purposes, Insider Subornation done generally for profit, Uncontrolled Secondary Usage, and Unauthorized Access. The NIST 800-30 provides a categorization of threat sources in six items: Human Deliberate, Human Unintentional, Technical, Operational, Environmental, and Natural [23].

Recent policy-based studies broadly categorize privacy threats, or source of information security, into two areas: Organizational and Systemic threats. Organizational threats are categorized into five levels: Accidental Disclosure, Insider Curiosity, Data Breach by Insider, Data Breach by Outsider with physical intrusion and Unauthorized Intrusion of Network System [6].

A classification for the threats of IS like HIS were offered by Whitman to twelve items. [24]. He identified the priority of expenditures and to protect IS against these threats by provided an online survey by asking IT executives to rank the threats to information security [24]. The findings showed that the most critical threat for IS is "Deliberate Software Attacks" which was weighted almost twice more important in comparison to the second threat on the list. Technical Software Failures or Errors, Acts of Human Error, Failure and Deliberate Acts of Espionage or Trespass were also noted as high-risk threats for the HIS [25].

Each organization will need to prioritize the threats it faces, based on the particular security situation in which it operates, its organizational strategy regarding risk, and the exposure levels at which its assets operate [26]. Therefore, another categorization scheme has been done that consists of fourteen general categories that represents clear and present dangers to an organizations people, information, and systems. The results are generally similar to previous studies in which Espionage or Trespass and Software Attacks remain at the top of the list and Human Error or Failure in the third position. After them, there are new options, which are added in the last category namely: Missing Inadequate or Incomplete Organizational Policy or Planning and Missing Inadequate or Incomplete Controls [27]. Yeh and Chang [25] also identify fifty fundamental security countermeasures commonly adopted to evaluate the adequacy of IS security into seven categories.

According to [26], the following list, the significant threats have been classified and ranked by Annual Computer Crime and Security Survey in 2008: denial of Service, Laptop Theft, Telecom Fraud, Unauthorized Access, Virus, Financial Fraud, Insider Abuse, System Penetration, Sabotage, Theft/loss of Proprietary Info, Abuse of Wireless Network, Web Site Defacement, Misuse of Web Application, Bots, DNS, Attacks, Instant Messaging Abuse, Password Sniffing, Theft/Loss of Customer Data [28]. Additionally, ISO/IEC 27002 also addresses eleven standard areas related to information security management [16].

Study done by Narayana Samy, *et al.* [11] discovered that there are altogether 22 types of threats to Total Hospital Information system (THIS) and listed the critical threats to HIS. A year later in another study, they tested the categorization listed in a hospital in Malaysia. The results showed the most critical threats along with the ranking of threats [29].

Pardue and Patidar [20] on other hand, represent a preliminary effort at cataloging threats to electronic healthcare data associated with unauthorized access, data loss, and data corruption, which caused by vandalism, loss or corruption of data, due to faulty hardware and software, human error, malware, natural disaster and database attack.

Another model [4] of the threat tree was organized around the goal of an attacker or outcome of a threat, depending on whether the threat is intentional or not.

Then Kotz [19] provided a taxonomy consisting of 25 threats, organized around three main categories: identity threats, access threats, and disclosure threats. Threats are organized by different types such as misuse of patient identities, unauthorized access or modification of Personal Health Information (PHI), or disclosure of PHI. Each category considers three types of the adversary: Patient himself or herself, Insiders (authorized Personal Health Record (PHR) users, staff of the PHR organization, or staff of other mobile health support system), and

Outsiders (third parties acting without authorization).

Another study mentions that most people are familiar with common types of computer security breaches that are caused by Computer Viruses, The Internet, Hackers, Worms, and Malicious Software Designed to compromise or disrupt other computer systems, and the loss or theft of laptops containing sensitive data. Security of the computers embedded in sophisticated medical devices, and unauthorized communication may increase susceptibility to security breaches [18]. **Table 1** summarizes and reviewed previous work done in identifying threats to HIS. Outstanding works are itemized from the year 1992 till 2011. All in all, thirty (30) threats were classified. It is noted that "deliberate acts of theft of data", "misuse of system resources", "users errors", "deviations in quality of service" are among the common threats to HIS.

Table 1. Summary of related works on threat to HIS.

Threats to HIS	Samy (2011)	Pardue (2011)	Sharma (2011)	Kohno (2010)	Whitman (2009)	Summer (2009)	Caballero (2009)	Richardson (2008)	Ilias (2006)	Whitman (2003)	Power (2002)	Rindfleisch (1997)	Loch (1992)
Power Failure/loss	√						√		√				
Network Infrastructure Failures or Errors	√						√	√	√		√		
Technological Obsolescence	√				√					√			
Hardware Failures or Errors	√	√			√		√		√	√			
Software Failures or Errors	√	√			√	√	√		√	√			
Operational Issues	√								√				
Communications Interception	√										√		
Repudiation	√												
Espionage or Trespass	√						√						
Communications Infiltration	√							√	√		√		
Social Engineering Attacks	√												
Technical Failure	√												
Deliberate Acts of Theft of Data	√		√		√		√	√	√	√	√		
Misuse of System Resources	√		√		√		√		√	√	√	√	√
Unauthorized Communication				√				√			√		
Staff Shortage	√								√				
User Errors	√	√	√		√	√	√	√	√	√		√	√
Sabotage or Willful Damages	√				√	√	√		√	√			
Environmental Threats	√						√		√				√
Deviations in Quality of Service	√	√	√	√	√	√	√	√		√	√	√	√
Maintenance Error									√				
Misuse of Web Application	√							√	√				
Compromises to Intellectual Property					√					√			
Missing, Inadequate or Incomplete Organizational Policy or Planning			√		√								√
Missing, Inadequate or Incomplete Controls			√		√							√	√
Financial Fraud							√	√			√	√	
Terrorism	√												
Unauthorized Access to Information Database		√	√					√			√	√	√
Natural Disasters		√	√		√		√	√	√	√			√
Theft of Equipment	√		√	√	√		√	√		√	√		

4. Research Methodology

This paper proceeds in describing how the data were collected. Secondary data resources aided in providing the relevant data in identify the threats to HIS. A thorough on-line search was carried out. Among the various search databases were ACM Digital Library, AISeL, EBSCO, IEEE Xplore, PUBMED, SPRINGER, ELSEVIER, and SCOPUS. Keywords such as “threats of health information systems”, “threats to health technology”, “threats to information systems”, and “electronic health” are input for the search. From the initial 30 common criteria, it was further breakdown 70 threats. **Table 2** depicts the detailed two-level categorization of threats.

Table 2. Threat tree for HIS.

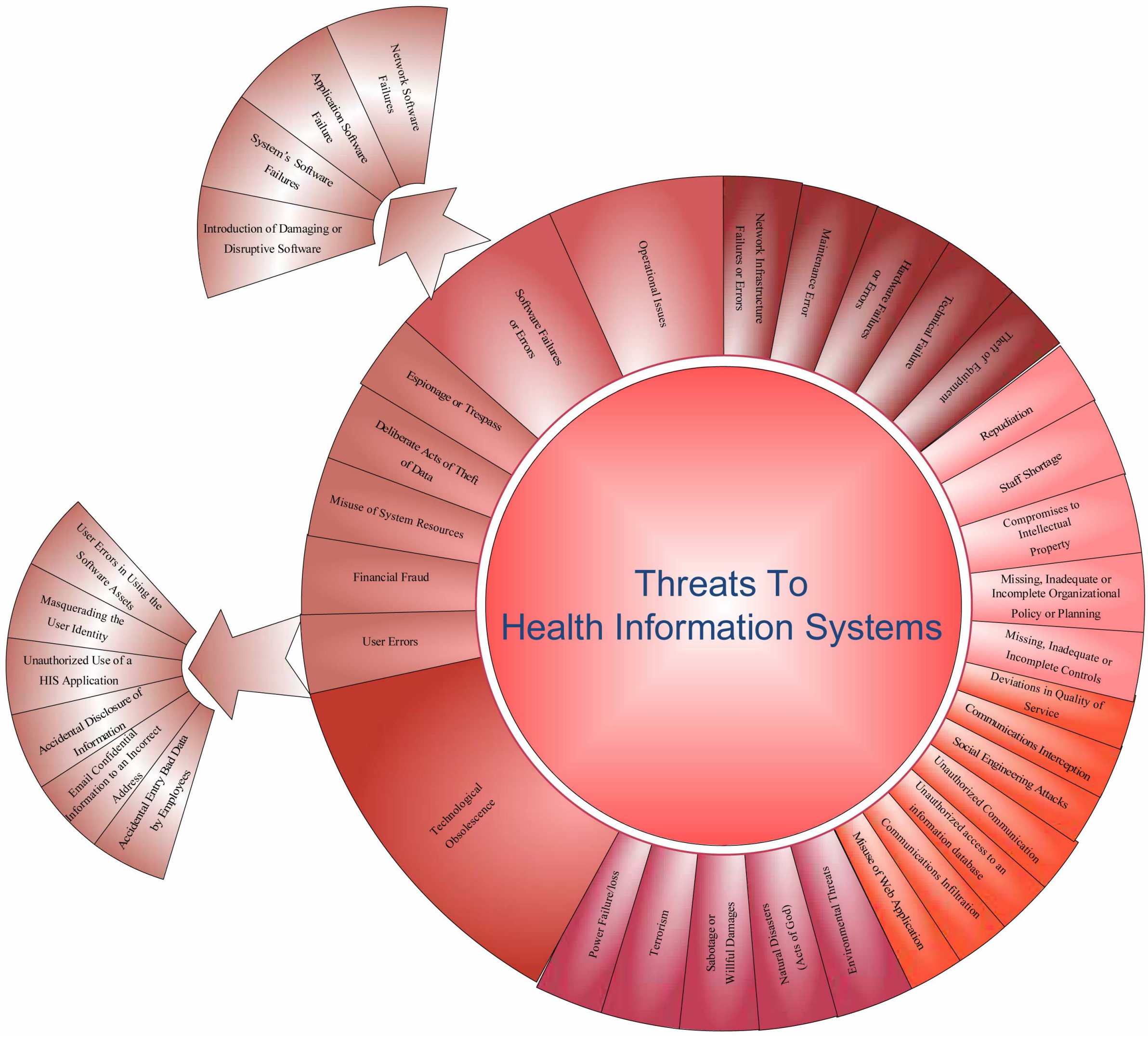
1. Power Failure/loss
1.1. Power Failure of Server
1.2. Power Failure of Workstation
2. Network Infrastructure Failures or Errors
2.1. Technical Failure of Network Interface
2.2. Technical Failure of Network Services
2.3. Abuse of Wireless Network
3. Technological Obsolescence
4. Hardware Failures or Errors
4.1. System’s Hardware Failures
4.1.1. Switch
4.1.2. Hub
4.1.3. Router
4.1.4. Server
4.1.5. Firewall
4.1.6. Others
4.2. Network‘s Hardware Failures
5. Software Failures or Errors
5.1. Introduction of Damaging or Disruptive Software
5.2. System’s Software Failures
5.3. Network‘s Software Failures
5.3.1. Bugs
5.3.2. Code Problems
5.3.3. Unknown Loopholes
6. Operational Issues
7. Communications Interception
8. Repudiation
9. Espionage or Trespass
10. Communications Infiltration
10.1. Device Reprogramming
10.2. Unauthorized Data Extraction
11. Social Engineering Attacks
12. Technical Failure
13. Deliberate Acts of Theft Data
13.1. Theft/loss of Customer Data or Proprietary Info
13.2. Illegal Confiscation of Equipment or Information
13.3. Dumping Physical Files with Critical Information in Public
14. Misuse of System Resources
14.1. Third Party
14.2. Information Extortion
15. Unauthorized Communication
16. Unauthorized Access to Information Database
17. Staff Shortage
18. User Errors
18.1. User Errors in Using the Software Assets
18.2. Masquerading the User Identity
18.3. Unauthorized Use of a HIS Application
18.4. Accidental Disclosure of Information
18.5. Email Confidential Information to an Incorrect Address
18.6. Accidental Entry Bad Data by Employees
19. Sabotage or Willful Damages
20. Natural Disasters (Acts of God)
20.1. Flood
20.2. Landslides
20.3. Earthquake
20.4. Electrical storms
20.5. Lightning
20.6. Tornadoes
20.7. Avalanches
21. Environmental Threats
21.1. Water Damage
21.2. Fire
21.3. Air-condition Failure
21.4. Pollution
21.5. Chemicals
21.6. Liquid Leakage
22. Deviations in Quality of Service
22.1. QoS Deviations from Service Providers
22.2. Deliberate Software Attacks
22.2.1. Nonetheless Purposeful, attempt to circumvent system security
22.2.2. Malicious Attempt to gain unauthorized access
22.2.2.1. Password Sniffing
22.2.2.2. Telecom Eavesdropping
22.2.2.3. Database Attack
22.2.2.4. Denial of Service
22.2.2.5. Web Site Defacement
22.2.2.6. Bots
22.2.2.7. DNS Attacks
22.2.2.8. Malware Attack
22.2.2.8.1. Worm
22.2.2.8.2. Trojan Horses
22.2.2.8.3. Spyware
22.2.2.8.4. Virus
22.2.2.8.5. Adware
22.2.2.8.6. Macros
23. Maintenance Error
23.1. Hardware
23.2. Software
23.3. Network
24. Misuse of Web Application
24.1. Cross Site Scripts
24.2. Information Leakage
24.3. SQL Injection
24.4. HTTP Response Splitting
25. Compromises to Intellectual Property
26. Missing, Inadequate or Incomplete Organizational Policy or Planning
27. Missing, Inadequate or Incomplete Controls
28. Financial Fraud
29. Terrorism
30. Theft of Equipment

5. Threat Tree for Risk Assessment

In order to protect the information in the organization, firstly, it is suggested to recognize the data protection and storage, transmission and processing systems. Secondly would be the category threats faced. So, information security personnel must be informed about the different threats to assets in information systems [27]. As for Health Information System there are six proposed components that include software, hardware, data, people, procedures, and networks. These six critical components enable information to be input, processed, output, and stored. Each of these IS components has some strengths and weaknesses, as well as characteristics and uses. Each component of the information system also has its own security requirements [27]. Therefore an organized classification of threats is required in order to discuss information security issues.

In this section authors propose a tree structure for cataloging threats to healthcare assets as a threat tree. The purpose of the threat tree presented here is to facilitate risk assessment and provision of the health care policy and legislation by using second data resources involves the use of different threat catalogs and literature to finding a comprehensive model which are shown in **Table 2**. The health information threat catalog has beneficial effects on risk assessment and needs categorization and documentation more than just what is shown in the **Table 2**. Risk assessment needs to provide the various sources of threats in HIS.

Each of the threats in the tree is used for providing a set of controls to decrease the risk of exploitation of vulnerability. It can also help analysts to assignment of threats as well as compare their assessment with the assessment of other analysts. From **Table 2**, we can represent the categorization in the pie format for better visualization and understanding. **Figure 2** also illustrates a simple view.



Network Software Failures
Application Software Failure
System's Software Failures
Introduction of Damaging or Disruptive Software
Operational Issues
Network Infrastructure Failures or Errors
Maintenance Error
Hardware Failures or Errors
Technical Failure
Theft of Equipment
Repudiation
Staff Shortage
Compromises to Intellectual Property
Missing, Inadequate or Incomplete Organizational Policy or Planning
Missing, Inadequate or Incomplete Controls
Deviations in Quality of Service
Communications Interception
Social Engineering Attacks
Unauthorized Communication
Unauthorized access to an information database
Communications Infiltration
Misuse of Web Application
Environmental Threats
Natural Disasters (Acts of God)
Sabotage or Willful Damages
Terrorism
Power Failure/loss
Technological Obsolescence
User Errors
Financial Fraud
Misuse of System Resources
Deliberate Acts of Theft of Data
Espionage or Trespass
Software Failures or Errors
Threats To Health Information Systems
User Errors in Using the Software Assets
Masquerading the User Identity
Unauthorized Use of a HIS Application
Accidental Disclosure of Information
Email Confidential Information to an Incorrect Address
Accidental Entry Bad Data by Employees

Figure 2. Simple model of threat tree for HIS.

6. Conclusion

This paper presents categorize different threats to healthcare information system. The identification of threat would play a role as an effective method in accessing security for risk management. The threat tree consolidated may provide initial step facilitating risk analysis process. Researchers and system developers may find this effort useful in the advancement of HIS security. Although this study attempts to provide a complete taxonomy for threats to HIS, it is still regarded as a work in progress as the research needs to proceed in ranking the potential security threats to HIS. Timely identification to threats is essential as technology improved and its assets progress.

7. Acknowledgements

This study was funded by the Research University Grant (RUG) from Universiti Teknologi Malaysia (UTM) and Ministry of Higher Education (MOHE) Malaysia with project number Q.K 130000.2138.01H98.

REFERENCES

[1] National Science Foundation, "Changing the Conduct of Science in the Information Age," 2011.

[2] H. Jahankhani, *et al*., "Security Risk Management Strategy: Handbook of Electronic Security and Digital Forensics," World Scientific, New Jersey, London and Singapore, 2009, p. 237.

[3] K. M. Albert, "Integrating Knowledge-Based Resources into the Electronic Health Record: History, Current Status, and Role of Librarians," *Medical Reference Services Quarterly*, Vol. 26, No. 3, 2007, pp. 1-19. doi:10.1300/J115v26n03_01

[4] J. P. Landry, *et al*., "A Threat Tree for Health Information Security and Privacy," *Proceedings of the* 17*th American Conference on Information Systems*, Detroit, 4-8 August 2011.

[5] C. A. Shoniregun, *et al*., "Introduction to e-Healthcare Information Security," *Electronic Healthcare Information Security*, Vol. 53, 2010, pp. 1-27. doi:10.1007/978-0-387-84919-5_1

[6] A. Appari and M. E. Johnson, "Information Security and Privacy in Healthcare: Current State of Research," *International Journal of Internet and Enterprise Management*, Vol. 6, No. 4, 2010, pp. 279-314. doi:10.1504/IJIEM.2010.035624

[7] HIMSS, "Kroll-HIMSS Analytics 2010 Report on Security of Patient Data," 2008.

[8] HIMSS, "Kroll-HIMSS Analytics 2010 Report on Security of Patient Data," 2010.

[9] G. N. Samy, *et al*., "Threats to Health Information Security," *Proceedings of the* 5*th International Conference on Information Assurance and Security of the IEEE IAS*, Xi'an, 8-20 August 2009, pp. 540-543. doi:10.1109/IAS.2009.312

[10] S. Kahn and V. Sheshadri, "Medical Record Privacy and Security in a Digital Environment," *IT Professional*, Vol. 10, No. 2, 2008, pp. 46-52. doi:10.1109/MITP.2008.34

[11] G. N. Samy, *et al*., "Security Threats Categories in Healthcare Information Systems," *Health Informatics Journal*, Vol. 16, No. 3, 2010, pp. 201-209. doi:10.1177/1460458210377468

[12] S. Samsuri, *et al*., "User-Centered Evaluation of Privacy Models for Protecting Personal Medical Information," *Informatics Engineering and Information Science*, Vol. 251, 2010, pp. 301-309. doi:10.1007/978-3-642-25327-0_26

[13] A. Ekelhart, *et al*., "AURUM: A Framework for Information Security Risk Management," *Proceedings of the* 42*nd Hawaii International Conference on System Sciences*, Hawaii, 5-8 January 2009, pp. 1-10. doi:10.1109/HICSS.2009.595

[14] Z. Ismail, *et al*., "Framework to Manage Information Security for Malaysian Academic Environment," *Information Assurance & Cybersecurity*, Vol. 2010, 2010, 16 p. doi:10.5171/2010.305412

[15] A. Yasinsac and J. H. Pardue, "A Process for Assessing Voting System Risk Using Threat Trees," *Journal of Information Systems Applied Research*, Vol. 4, No. 1, 2010, pp. 4-16.

[16] R. Gomes and L. V. Lapão, "The Adoption of IT Security Standards in a Healthcare Environment," *Studies in Health Technology and Informatics*, Vol. 136, 2008, pp. 765-770.

[17] M. Sumner, "Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness," *Information Systems Management*, Vol. 26, No. 1, 2009, pp. 2-12. doi:10.1080/10580530802384639

[18] W. H. Maisel and T. Kohno, "Improving the Security and Privacy of Implantable Medical Devices," *New England Journal of Medicine*, Vol. 362, 2010, pp. 1164-1166. doi:10.1056/NEJMp1000745

[19] D. Kotz, "A Threat Taxonomy for mHealth Privacy," *Proceedings of the* 3*rd International Conference on Communication Systems and Networks of the IEEE COMSNETS*, Bangalore, 4-8 January 2011, pp. 1-6. doi:10.1109/COMSNETS.2011.5716518

[20] J. H. Pardue and P. Patidar, "Thrats to Healthcare Date: A Threat Tree for Risk Assessment," *Issues in Information Systems*, 5-8 October 2011.

[21] R. Power, "CSI/FBI Computer Crime and Security Survey: Computer Security Institute," SCI & FBI, 2002.

[22] T. C. Rindfleisch, "Privacy, Information Technology, and Health Care," *Communications of the ACM*, Vol. 40, No. 8, 1997, pp. 92-100. doi:10.1145/257874.257896

[23] G. Stonebumer, *et al*., "Risk Management Guide for Information Technology Systems," National Institute of Standards and Technology, 2002.

[24] M. E. Whitman, "Enemy at the Gate: Threats to Information Security," *Communications of the ACM*, Vol. 46, 2003, No. 8, pp. 91-95. doi:10.1145/859670.859675

[25] M. E. Whitman, "In Defense of the Realm: Understanding the Threats to Information Security," *International Journal of Information Management*, Vol. 24, No. 1, 2004, pp. 43-

57. doi:10.1016/j.ijinfomgt.2003.12.003

[26] M. E. Whitman and H. J. Mattord, "The Enemy Is still at the Gates: Threats to Information Security Revisited," *Proceedings of the* 2010 *Information Security Curriculum Development Conference*, Kennesaw, 1-3 October 2010, pp. 95-96. doi:10.1145/1940941.1940963

[27] M. E. Whitman and H. J. Mattord, "Principles of Information Security," Course Technology Ptr, Boston, 2011.

[28] R. Richardson, "CSI Computer Crime and Security Survey," Computer Security Institute, 2008, pp. 1-30.

[29] G. N. Samy, *et al*., "Health Information Security Guidelines for Healthcare Information Systems," Zurich, 8-9 September 2011, p. 10.