Threats to Health Information Security

Ganthan Narayana Samy  
Department of Computer Systems and Communications  
Faculty of Computer Science and Information Systems  
Universiti Teknologi Malaysia (UTM)  
Malaysia  
ganthan2@siswa.utm.my

Rabiah Ahmad  
Centre for Advanced Software Engineering (CASE)  
Faculty of Computer Science and Information Systems  
Universiti Teknologi Malaysia (UTM)  
Malaysia  
rabiah@citycampus.utm.my

Zuraini Ismail  
Department of Science  
College of Science and Technology  
Universiti Teknologi Malaysia (UTM)  
Malaysia  
zurainisma@citycampus.utm.my

Abstract— The purpose of this paper is to identify the threats that exist in Healthcare Information Systems (HIS). The study has been carried out in three different departments namely, Information Technology Department (ITD), Medical Record Department (MRD) and X-Ray Department in one of the leading government supported hospital in Malaysia. The hospital was equipped with Total Hospital Information System (THIS) environment. The data were collected using in-depth structured interviews. The study identified 22 types of threats according to major threat categories based on ISO/IEC 27002 (ISO 27799:2008). The result shows the most critical threat for the THIS is the power failure. In addition, acts of human error or failure threat also show high frequency of occurrence. The contribution of the paper will be categorization of threats in HIS and can be used to design and implement effective security systems and policies in healthcare setting.

Keywords-Threats, Healthcare Information Systems (HIS), Information Security, Risk Analysis.

I. INTRODUCTION

Nowadays, using information systems in the healthcare environment provides many potential benefits such as improving the quality of care, reducing medical errors, enhancing the readability, availability and accessibility of information [1]. However, Healthcare Information Systems (HIS) security threats have increased significantly in recent years. For instance, during the period from 2006 to 2007, over 1.5 million names were exposed during data breaches that occurred in hospitals alone [2]. Therefore, storing health information in electronic form raises concerns about patient’s health, privacy and safety. Basically, HIS are threatened by both accidental events and deliberate actions threats, which can severely damage health information systems’ reliability and consequently discourage professionals of future use. [3][4].

Furthermore, lack of adequate protection in sustaining the confidentiality, integrity and availability aspects leads for investigation to the potential threats particularly in healthcare information systems domain. Besides that, poor organization of security measures or low awareness of risk analysis practices within public and private sector especially in healthcare organizations also need particular attention. Further investigation to identify security threats in healthcare information systems is mandatory. Additionally, lack of “good industry practices” or standards for instance, ISO/IEC 27002 (ISO 27799:2008) or Health Insurance Portability and Accountability Act (HIPAA) in healthcare environment is urgently required in order to protect the computerized information assets. For these reasons, this study was carried out in one of the leading government supported hospital in Malaysia.

This paper is organized as follows. The next section describes the previous studies related to this research. Section III explains research method used in this research. Section IV presents the results of the studies. Section V presents the discussion, followed by conclusion in section VI.

II. RELATED STUDIES

According to International Standard for Health Informatics for Information Security Management in Health using ISO/IEC 27002 (ISO27799:2008), defined HIS as a repository of information regarding the health of a subject of care in computer-process able form, stored and transmitted securely and accessible by multiple authorized users [5]. There are various types of threats categories introduce by standards and authors. Basically, this standard classified threats to HIS into 25 types.

Besides that, [6] have been classified threats to information system at hospital into two main categories, namely, internal threats and external threats. An internal
threat includes various types of employees’ behavior such as employee’s ignorance, curiosity, recklessness, inadequate behavior, taking someone else’s password and giving password to another employee. For an external threat includes viruses and spyware attacks, hackers and intruders in premises.

Besides that, [3] has categorized HIS threats into 19 types based on case study conducted using a selected risk analysis method. The findings shows that the most critical threat for the HIS is the power failure of the server. Furthermore, power failure of the workstation, system and network software failure and tele-monitoring software failure also presents high-risk threats for the HIS. Besides that, there are also a number of highly risk threats related to the human factor, such as user errors in using the software assets of the HIS and masquerading the user identity during system operation.

Furthermore, another study has categorized 25 types of threats to patient monitoring system [7]. The most critical threat is the power failure of the server, while the power failure of the home personal computer is the second most critical failure for the system. Furthermore, air-conditioning failure, system and network software failure, monitor support software failure and medical record software failure also treated as high-risk threats for this system. However, this study also identified a number of high-risk threats related to the human factor, such as user errors in using the software assets and masquerading.

III. RESEARCH METHOD

This study was conducted from August to September 2008 at one of the government supported hospital in Peninsular Malaysia. The hospital has 960 inpatient beds and 20 clinical disciplines. This hospital provides secondary and selected national tertiary care services. It consists of centre for Gastroenterology, Rheumatology, Hepatology, Hepatobiliary surgery, Vitreoretinal surgery, Colorectal surgery, Microsurgery, and Renal service. Furthermore, being a referral hospital it provides specialist outpatient service for referred cases. This hospital has been designed, constructed and equipped for a Total Hospital Information System (THIS) environment. This is the first hospital in Malaysia and in the world to operate with THIS covering all aspects of its operation. The ultimate aim of this hospital is to be paperless and filmless operation hospital.

A. Structured Interview

In order to gain a better and in-depth understanding of the context, and potential factors or threats, which might influence the HIS, a structured interview approach was used. Moreover this approach can encourage interaction with real users to explore their perspectives towards an information system, which in turn, can help to improve the design and usability of the system [1][8].

B. Participant’s Characteristics

16 staffs from three different departments were interviewed in total. Eleven participants from Information Technology Department (ITD), four participants from Medical Record Department (MRD) and only one participant from X-Ray Department. Six of the participants were male and ten participants were female. The age range was 24-55 years old. Basically, their duration of employment in that particular department was similar, ranging from six months to more than nine years. Basically participants were categorized according to five professional communities based on position. Two Managers, two Information System Professionals, five Information System Technicians, three Nurses (various grades) and four Clerks.

In order to maintain the confidentiality of the participants’ information during data analysis and in reporting the findings, the identities of the participants were anonymised.

C. Data Collection and Analysis

Before undertaking interview, an information sheet was given to the interviewees to inform them about the study and the process of the interview as well as to get confirmation from the interviewees to be interviewed. In this study, interview participants are invited, who representing by different position levels from three different departments namely, Information Technology Department (ITD), Medical Record Department (MRD) and X-Ray Department. The interview guide focused on few questions, such as: What are the threats to Healthcare Information Systems? Which of these threats are the most serious to Healthcare Information Systems? How frequently are these threats observed? The mean length of interview was 51 minutes.

IV. RESULTS

A. Total Hospital Information System (THIS) Environment

The Total Hospital Information System is an integration of clinical, administrative and financial systems. The clinical is made up of Hospital Information System and Picture Archiving Communication System (PACS). The Hospital Information System is made up of various applications such as person management, scheduling, order management and clinical documentation. The administration and finance system as back end which is integrated with the Hospital Information System so that any chargeable procedures or tests performed on the patients will automatically trigger the generation of the bills. With PACS, the system is also interfaced with the various x-ray machines.

Therefore, the challenge here is that the integration is so deep and extensive that it is not only between software applications but also between applications and equipment especially in the radiology, laboratory, intensive care and operating theatres where the system is interfaced directly into the equipment and whatever data or image produced by
such equipment will go directly on-line into the system. In conclusion, patients' medical records, guidelines and clinical protocols are instantly available and can be assessed in one integrated workstation at any place and at any time in the hospital, provided that the user has proper authority to access the information. Therefore, security is very important and plays a vital role in protecting THIS asset and information.

B. Threats Identified in THIS

The key information sought in this study is identification of threats in THIS. Table I depicts 22 types of threats according to major threat categories. Basically, the threats were categorized based on relevant standards [5][9] and also based on a comparative study of previous works and publications [10][11][12][13][14] as well as based on case study conducted in this research.

Table II presents the most critical threats in THIS with description. The study shows the most critical threat for the THIS is the power failure. This is due to power failure of server, air-conditioning failure or interruption by service providers. Besides that, acts of human error or failure threat also show high frequency of occurrence in THIS. Furthermore, in acts of human error threat, one of the greatest threats to HIS is the entry of erroneous data by staff. Basically, such a threat represents a serious threat to the confidentiality, integrity and availability of data. This kind of incidents happens due to lack of awareness and good practices among the staff.

Besides that, technological obsolescence also considered as one of critical factors to THIS. Basically, technological obsolescence referring to antiquated or outdated infrastructure such as hardware, application software and network equipment which can lead to unreliable and untrustworthy systems.

In addition, other category of threats namely hardware failures or errors and software failures or errors also give significant value. These defects can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability.

V. DISCUSSION

The study shows the most critical threat for the THIS is the power failure. Similarly, previous studies also found power failure is one of the most critical threats to HIS [3][7]. Besides technological factors, non technological factors such as human error also consider as important threats in HIS [2]. Thus, human error or failure can be prevented with appropriate security education, training and awareness programs. Therefore, this study has proven useful in identifying critical threats to HIS, and could be useful especially for information security officers or policy maker to get clear understanding in order to design and implement effective security systems and policies.

Besides that, the most important contribution of this paper will be threats categorization in HIS which was not only based on relevant standards but also referring publications as well as based on real case study which was conducted in this research in order to identify the threats to HIS. Thus, this paper provides a description and understanding of broad categories of potential threats in HIS. Furthermore, this threats categorization will be useful in order to develop a greater degree of awareness and understanding of security threats associated with patient data particularly, for healthcare professionals and employees, those who are working in healthcare industry. Moreover, these findings will enable us to identify the overall risks in HIS and subsequently develop a sound remediation plan.

### Table I. Threats to THIS

<table>
<thead>
<tr>
<th>No.</th>
<th>Categories of Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power failure/loss</td>
</tr>
<tr>
<td>2</td>
<td>Network Infrastructure failures or errors</td>
</tr>
<tr>
<td>3</td>
<td>Technological Obsolescence</td>
</tr>
<tr>
<td>4</td>
<td>Hardware failures or errors</td>
</tr>
<tr>
<td>5</td>
<td>Software failures or errors</td>
</tr>
<tr>
<td>6</td>
<td>Deviations in quality of service</td>
</tr>
<tr>
<td>7</td>
<td>Operational issues</td>
</tr>
<tr>
<td>8</td>
<td>Malware attacks (Malicious virus, Worm, Trojan horses, Spyware and Adware)</td>
</tr>
<tr>
<td>9</td>
<td>Communications interception</td>
</tr>
<tr>
<td>10</td>
<td>Masquerading</td>
</tr>
<tr>
<td>11</td>
<td>Unauthorized use of a health information application</td>
</tr>
<tr>
<td>12</td>
<td>Repudiation</td>
</tr>
<tr>
<td>13</td>
<td>Communications infiltration</td>
</tr>
<tr>
<td>14</td>
<td>Social Engineering attacks</td>
</tr>
<tr>
<td>15</td>
<td>Technical failure</td>
</tr>
<tr>
<td>16</td>
<td>Deliberate acts of Theft (including theft of equipment or data)</td>
</tr>
<tr>
<td>17</td>
<td>Misuse of system resources</td>
</tr>
<tr>
<td>18</td>
<td>Acts of Human Error or Failure</td>
</tr>
<tr>
<td>19</td>
<td>Staff shortage</td>
</tr>
<tr>
<td>20</td>
<td>Wilful damages</td>
</tr>
<tr>
<td>21</td>
<td>Environmental Support Failure/Natural disasters</td>
</tr>
<tr>
<td>22</td>
<td>Terrorism Attacks</td>
</tr>
</tbody>
</table>
TABLE II. MOST CRITICAL THREATS TO HIS

<table>
<thead>
<tr>
<th>No.</th>
<th>Categories of Threat</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1   | Power failure/loss   | - Server down due to power failure  
- Air-conditioning failure of the server  
- Interruption by service provider (e.g. Electrical Department & Internet Service Provider) |
| 2   | Acts of Human Error or Failure | - Entry of erroneous data by staff  
- Accidental deletion or modification of data by staff  
- Accidental misrouting by staff  
- Confidential information being sent to the wrong recipient  
- Storage of data/ classified information in unprotected areas by staff |
| 3   | Technological Obsolescence | - Outdated Hardware  
- Outdated application software  
- Outdated system software  
- Obsolete network equipment |
| 4   | Hardware failures or errors | - Insufficient storage space  
- Hardware maintenance error |
| 5   | Software failures or errors | - Application software failure  
- Software maintenance error |

VI. CONCLUSION

The most important findings of the analysis are threats categorization particularly in HIS. Therefore, this research holds significant guideline for information security practitioners or top level management when making investment for information security management and able to manage their HIS effectively. Ultimately, this ongoing research work intends to develop appropriate information security policy framework for HIS.

ACKNOWLEDGMENTS

We gratefully acknowledge the funding received from Ministry of Science, Technology and Innovation (MOSTI) that helped sponsor this research study and also sincere thanks for the cooperation given by Ministry of Health Malaysia, Hospital Selayang and Universiti Teknologi Malaysia (UTM).

REFERENCES