Development of a Security Information System in a Hospital

Bobi Kurniawan [1], Ricky Nugraha [2]
{bobi@unikom.ac.id[1], rickynugraha@mahasiswa.unikom.ac.id[2]}

Fakultas Teknik dan Ilmu Komputer, Universitas Komputer Indonesia, Indonesia[1], Fakultas Teknik dan Ilmu Komputer, Universitas Komputer Indonesia, Indonesia[2].

Abstract. The purpose of this study was to identify technological developments in information security systems in hospitals. The method used in this study was a review method with techniques for reviewing and analyzing several papers related to the topic of discussion about the safety of hospital information systems. The results of the study are that the highest threat to the security of hospital information systems is the threat of hackers. The development of technology makes it easy for people, especially in business. In general, this research is in accordance with the expected objectives, namely, to know the security of the health information system network.

Keywords: Information System, Development, Hospital.

1 Introduction

John F. Nash explained that information systems are a combination of human, technological facilities, tools, media, procedures and controls aimed at regulating important communication networks, certain transaction processes and routines, helping internal and external management and users and providing a basis for retrieval the right decision [1]. Likewise with Robert A. Leitch and K. Roscoe Davis who explained about information systems is a system in an organization that brings together daily transaction processing needs, supports operations, managerial and strategic activities of an organization and provides certain external parties with reports that needed [2].

GJ Simons explained that the security of information systems is how we can prevent cheating or at least detect fraud in an information-based system, where the information itself does not have a physical meaning, but information system security can be interpreted as a technical policy, procedure and measurement used to prevent unauthorized access, program changes, theft or physical damage to the information system. Safeguards against information technology can be improved by using techniques and equipment to secure computer hardware and software, communication networks and data [3].

Kroll Fraud explained that using information systems in health services can provide many potential benefits such as improving service quality, reducing medical errors, increasing reading of availability of facilities and accessibility of information. However, the threat to the health of the health information system also increased significantly. For example, during the 2006-2007 period, there were more than 1.5 million data errors that occurred in hospitals [4]. Research conducted by Elias found that storing health information in electronic form can cause concerns for patients and hospital management. Basically, intentional threats and actions can seriously

INCITEST 2019, July 18, Bandung, Indonesia

DOI 10.4108/eai.18-7-2019.2287713

damage the health information system and consequently can prevent professionals from using it later [5]. Compared with a study conducted by Abdurrahim on the analysis In Bogor found different results of research conducted by Abdurrahim found that health information factors in electronic form did not affect patients and hospital management [6]. Research conducted by ISOt on the security of information systems is all forms of mechanisms that must be carried out in a system that is shown so that the system is protected from all threats that endanger the data security of information and security of system actors [7]. Samy, G.N and all explained that the lack of adequate protection in supporting aspects of confidentiality, integrity and availability for investigation also posed a threat, especially in the health information system domain. This requires more management in information security and special attention from the public and private sectors. Further investigation is needed to identify the threats to health information system security is mandatory. A good industrial practice or standard is needed in the development of information systems [8]. Besides, Samy, G.N and all describe that threats include various types of employee behavior such as employee ignorance, carelessness, taking other employee passwords and providing passwords for other employees. For external threats, namely viruses and spyware attacks, hackers and intruders in place. In addition, the threat of hospital information systems has been categorized based on case studies conducted using the risks chosen in the analysis method. [9]. Furthermore, power failures from system workstations and telemonitoring software and software network failures are high-risk threats to information systems [10, 11].

The purpose of this study is to identify threats information system security in hospitals, and the benefits of applying a security information system to hospitals. The method used in this study was a review method with techniques for reviewing and analyzing several papers related to the topic of discussion about the safety of hospital information systems.

2 Methods

This research was carried out by conducting a review of several papers that paid attention to the security of hospital information systems. Furthermore, after conducting a review, a grouping of what is a threat to the health information system is carried out. Finally, the discussion was carried out on the results of the groupings obtained. For example can be seen in figure 1.

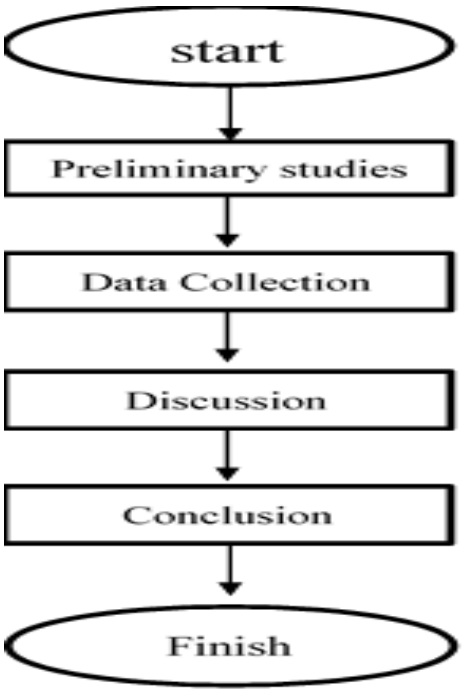

Fig 1. Flow of Research Methodology

3 Results And Discussion

In the review, several references were chosen from various sources. Table 1 shows some references that were used as material for review in this study. as an example can be seen in Table 1.

Table 1. List of references reviewed

No	Title	Author
1	Modeling risk in distributed healthcare information systems	Maglogiannis, Ilias
2	Security of Patient Data	Kroll Fraud Foundation
3	Analisa Database dan Keamanan Sistem Informasi	Abdurrahim
4	Threats to Health Information Security	Samy, G.N., Rabiah Ahmad., Zuraini Ismail
5	Information Security Management in Health	ISO 27799:2008
6	An Integrated Approach in Risk Management Process for Identifying Information Security	Samy, G.N., Rabiah Ahmad., Zuraini Ismail
7	Practical UNIX & Internet Security	G.J Simson, dan gene Spafford

The first paper identifies threats to health information system security in the form of user negligence (user), viruses, hackers (hackers), spyware attacks, server power failures, workstation system power failure and intrusion / theft. Then the second paper identified the threat to health information system security in the form of malcious code, viruses, social engineering, hackers, and theft. Furthermore, the third material identifies threats to the security of the health information system in the form of data theft, activity, espionage, hackers and acts of vandalism.

In the fourth paper, the study identifies threats to health information system security in the form of malicious code, viruses, social engineering, hackers, and theft and is also influenced by natural threats such as water threats, land threats and other threats such as fire, lightning. Furthermore, the sixth paper identifies threats to the security of health information systems in the form of malicious code, viruses, social engineering, hackers, and theft. Then the fifth source is reviewed, identifying threats to the health of the health information system in the form of malicious code, viruses, social engineering, hackers, and theft. Lastly the seventh paper identifies threats to health information system security in the form of malicious code, viruses, social engineering, hackers, and theft and is also influenced by natural threats such as water threats, land threats and other threats such as fire, lightning. Table 2 shows the results of the threat modeling that appears as a concern for the papers reviewed. Grouping is carried out based on grouping carried out by one of the existing papers.

Based on the results of reviews of various papers, the threat that often occurs comes from hackers. The threat posed by hackers to the information system is because an information system for companies or individuals is used to store important data concerning the privacy or confidentiality of the company. Especially companies that use the web, are very vulnerable to abuse because on a web can be accessed by everyone, the threat of hackers becomes very potential when there is no physical limit and control is done centrally. Then the development of a very fast network also contributes to differences in security skills, where experts will threaten the less skilled. as an example can be seen in table 2.

Table 2. List of threats presented in each paper

	Threat category	Paper						
		1	2	3	4	5	6	7
1.	Human Threat	√						
a.	Employee Ignorance	√						
b.	Employee Carelessness	√						
c.	Server Power Failure	√						
d.	Malicious Code		√		√	√	√	√
e.	Virus	√	√		√	√	√	√
f.	Spyware Attack	√						
g.	Hacker	√	√	√	√	√	√	√
h.	Social Engineering		√		√	√	√	√
i.	Theft	√	√		√	√	√	√
j.	Copy without permission							
k.	Information war							
l.	Data Theft			√				
m	Espionage activity			√				
n.	Act of Vandalism			√				
2.	Natural Threat							
a.	Water Threat		√	√	√	√	√	√

	Threat category	Paper						
		1	2	3	4	5	6	7
b.	Land Threat		√	√	√	√	√	√
c.	Wind Threat		√	√	√	√	√	√
d.	Lightning		√	√	√	√	√	√
e.	Fire		√	√	√	√	√	√
3.	environmental threat							
a.	Electric voltage drop		√		√	√	√	√
b.	Pollution		√		√	√	√	√
c.	Chemical Effects		√		√	√	√	√
d.	Leakage.		√		√	√	√	√

For threats caused by nature are water threats, land threats, wind threats and other threats such as lightning and fire. Because by sometimes not considering the threat of this nature. In addition, the threat of computer viruses is also the result of the work of a programmer who has evil intentions or only to satisfy the lust of his programming that successfully infiltrated the virus into other people's computer systems. The virus infiltrated the computer system in various ways, including:

- Exchange files, for example taking files (copy-paste) from other computers that have contracted the virus.
- Email, reading emails from unknown sources can risk contracting the virus, because the virus has been added (attached) to the e-mail file.
- IRC, chat channels can be used as a way for viruses to enter the computer.
- By looking at some aspects that pose a threat to the security of the health information system presented in the papers reviewed, several things that need to be considered by the information system manager are:
    - Perform adequate protection in supporting aspects of confidentiality, integrity and availability for investigation. Further investigation to identify security threats in health information systems.
    - Conduct protection regarding policies, procedures, processes and activities to protect information from various types of threats.
    - Conduct security risk analysis to protect information assets to ensure information system security.

4 Conclusion

The development of technology makes it easy for people, especially in business. In general, this research is in accordance with the expected objectives, namely, to know the security of the health information system network. The results of various reviews of several papers, discussions and analysis can be concluded that the highest threat to health information system security is the threat of hackers.

References

[1] F Nash, John, Accounting Information System I Pratika Manual Approach Preparation of Methods and Procedures. (2003)
[2] Leitch Robert A., K. Roscoe Davis. Analisis & Desain. (2005)
[3] G.J Simson, dan gene Spafford, Practical UNIX & Internet Security, O'Reilly & Associates, Inc,2 nd edition, (1996)
[4] HIMSS Analytics, Kroll Fraud Foundation. HIMSS Analytics Report: Security of Patient Data. Chicago, IL : HIMSS Analytics. (2008)
[5] Maglogiannis, Ilias. Elias Zafiropoulos. "Modeling risk in distributed healthcare information systems", The 28th Annual International Conference of the IEEE on Engineering in Medical and Biology Society (EMBS), IEEE. (2006)
[6] Abdurrahim, M.F.H. Analisa Database dan Keamanan Sistem Informasi SUP Fatmawati. Bogor: IPB. (2011)
[7] ISO. ISO 27799:2008 about Health Informatics – Information Security Management in Health using ISO/IEC 27002. Geneva : ISO. (2008)
[8] Samy, G.N., Rabiah Ahmad., Zuraini Ismail. Threats to Health Information Security: Fifth International Conference on Information Assurance and Security. Malaysia : Universiti Teknologi Malaysia (2009).
[9] Samy, G.N., Rabiah Ahmad., Zuraini Ismail. An Integrated Approach in Risk Management Process for Identifying Information Security Threats using Medical Research Design. Malaysia : Universiti Teknologi Malaysia (2012).
[10] Eddy Soeryanto Soegoto.Entrepreneurship Menjadi Pebisnis Ulung.Jakarta :Elex. (2014)
[11] Iskandar, M. S., & Firdaus, I. N. (August). Marketing Strategy of Tourism Package through Design of Web-based Information System on One of Tours and Travel in Bandung. In IOP Conference Series: Materials Science and Engineering (Vol. 407, No. 1, p. 012048). IOP Publishing. (2018)