Threats On Accounting Information Systems

Azhar Susanto

Abstract: Accounting Information System is a component of an organization that collects, classifies, processes, and communicates financial information and decision making that is relevant to external parties and external parties. This study aims to find out the threats to the security of accounting information systems. This study uses a review method with the technique of reviewing and analyzing several papers related to the topic of discussion about the security of accounting information systems. The results of this study are that the highest threat to the security of accounting information systems is the threat of hackers.

Index Terms: Security Threats, Accounting Information System, Review, Information Systems

1 INTRODUCTION

Society has increasingly relied on accounting information systems, which have developed increasingly complex to meet the increasing need for information. In line with the increase in system complexity and dependence on the system, companies face an increased risk of the system being negotiated. Almost every year, more than 60% experience a major failure in controlling the security and integrity of computer information systems. The causes are as follows: information is available for a very large number of employees and information distributed in the information network is difficult to monitor; Society has increasingly relied on accounting information systems, which have developed more complex to meet the increasing need for information. Increased system information threats occur because the client/server system distributes data to many users, which is why the system is more difficult to control than the main computer system that is centralized and information is available to workers who are not good. An accounting information system as an open system cannot be guaranteed as a system that is free from errors or fraud. Good internal control is a way for the systems to protect themselves from harmful actions. The concept of control is increasingly important and occupies a strategic position because the threat to the Accounting Information System increases both in terms of type and intensity. In line with the increase in complexity and dependence systems on the system, companies face increased risk for systems that are being developed and negotiated. The potential for unexpected events or activities that cannot endanger both the accounting and organizational information systems are referred to as threats. The study was conducted by reviewing several papers relating to the attention of developers to the threat of accounting information system security.

2 LITERATURE REVIEW

Information system security is any form of mechanism that must be carried out in a system that is intended to prevent the system from all threats that endanger the data security of information and security of system perpetrators.

- *Azhar Susanto*
- *Accounting Department, Faculty of Economics and Business, Padjadjaran University, Bandung, Indonesia*

Threats include various types of employee behavior such as employee ignorance, carelessness, taking other employee passwords and providing passwords for other employees. Threats that may arise from information processing activities can come from nature, namely: water threats, land threats, and natural threats such as: forest fires, lightning, tornadoes, hurricanes, and so on.

Threat-1 for accounting information systems: Destruction due to Natural Disasters and Politics One of the threats faced by companies is due to natural and political disasters, such as fires, excessive heat, floods, earthquakes, wind storms, and war. Disasters that cannot be predicted can completely destroy the information system and cause a downfall of a company. When a disaster occurs, many companies are affected at the same time.

Threat-2 of Accounting Information Systems: Error in software and malfunction of equipment. The second threat to the company is software errors and equipment malfunctions, such as hardware failures, errors or software malfunctions, operating system failures, electrical interference and fluctuations, and undetected data transmission errors.

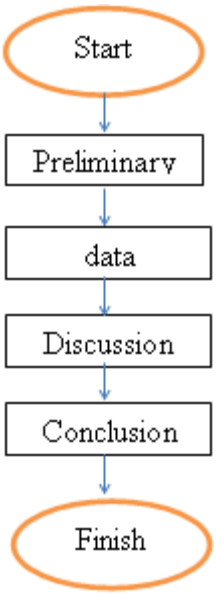
Threat-3 of the Accounting Information System: Accidental actions A third threat to companies is unintentional actions, such as errors or deletions due to ignorance or accident. This usually happens due to human error, failure to follow established procedures, and personnel who are not supervised or trained properly. Users often lose or misplace data, and accidentally delete or change files, data and programs. Computer operators and users can enter incorrect or unreliable input, use the wrong version of the program, use the wrong data file, or put the file in the wrong place. Analysts and system programmers make mistakes in the logic of the system, develop systems that do not meet the needs of the company, or develop systems that are unable to handle the tasks assigned.

Threat-4 of Accounting Information Systems: Accidental Actions (computer crime) The fourth threat facing the company is intentional action, which is usually referred to as computer crime. This threat is in the form of sabotage, the purpose of which is to destroy the system or some of its components. Computer fraud is another type of computer crime, with the aim of stealing valuable objects such as money, data, or computer time / services. This fraud can also involve theft, namely theft or improper use of assets by employees, accompanied by falsification of records to hide theft. The quality accounting information system is a quality accounting

information system (Sacer et al, 2006: 6). The fundamental role of accounting in organizations is to produce quality accounting information (Azhar Susanto, 2008: 374). The terms "quality" can mean success / success (Dellon & McLean, 2003), or effectiveness (Flyn, 1992), or user satisfaction (Stair & Reynolds, 2012). Whereas Gelinas et al (1990) use the term "effectiveness" accounting information system as a measure of the success of information systems in achieving the stated goals. Likewise, Flyn (1992) states that the effectiveness of SIA is acceptable to provide management information to assist management in making decisions. Delon & McLean (2003) uses the term "success" of the information system to measure the output produced by the real system. Likewise Pornpandejwittaya and Pairat (2012) use the term "success" in terms of the organization, used widely by one or more satisfied users and improve the quality of its performance. The term "quality" accounting information system proposed by Sacer et al (2006: 62) is used: hardware, software, brainware, telecomunication network, and a quality data base, as well as quality of work and satisfaction of users. Based on the description above, the use of the term "quality" as a synonym for the term "success", the Quality of Accounting Information System is reliably, efficiently and effectively as a provider of quality accounting information.

3 RESEARCH METHODOLOGY

This research was conducted by reviewing several papers that pay attention to the security threats of the accounting information system. Furthermore, after conducting a review, a grouping of what is a threat to the accounting information system is carried out. The research methodology is made in several steps as in Figure 1.



4 RESULT AND DISCUSSION

Based on the results of reviews of various papers, the threat that often occurs comes from hackers. The threat of hackers becomes very potential when there are no physical limits and controls are centralized. Threats to the security of accounting information systems can be in the form of user negligence, employee ignorance, employee carelessness, hacker virus, spyware attack, server power failure, malicius code, data theft, espionage activity, social engineering, workstation system power failure, copying without permission, information warfare, data theft, decrease in electricity voltage, pollution, chemical effects, leakage and theft and are affected by natural threats such as water threats, land threats and other threats such as fires and lightning. The threat of a computer virus is the result of the work of a programmer who has malicious intent or just to satisfy the lust of programming that successfully infiltrated the virus into someone else's computer system. Viruses infiltrate the computer system through various methods, including:

1. Exchange files, for example copy-paste from other computers that have contracted the virus.
2. E-mail, reading e-mails from unknown sources can risk contracting the virus, because the virus has been attached to an e-mail file.
3. 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 reviewed papers, several things that need to be considered by the information system manager are:

1. Conduct a security risk analysis to protect information assets.
2. Carry out safeguards regarding policies, procedures, processes and activities to protect information from various types of threats.
3. Conduct adequate protection in supporting aspects of confidentiality, integrity and availability for investigation.

5 CONCLUSION

The results of several papers review, discussion and analysis can be concluded that the highest threat to the security of accounting information systems is the threat of hackers. Some reasons for increasing security/threat issues in the accounting information system are as follows:

1) Increasing the number of client/server systems (client/server system) means that information is available to workers who are not good.
2) Pressure on productivity and costs makes management take time-consuming measures of control.

ACKNOWLEDGMENT

The authors wish to thank Padjadjaran University, Bandung Indonesia, and special thanks to Dr. Meiryani, Binus University, Jakarta, Indonesia.

REFERENCES

[1] Abdul Kohar and Hanson Prhihantoro Putro. (2014). Security Threats to Hospital Management Information Systems. 2014 National Informatioka Medical Seminar (SNIMed) V. 6 December 2014.

[2] Abdurrahim, M.F.H. (2011). Database Analysis and Information System Security. SUP Fatmawati. Bogor: IPB.

[3] ISO (2008) ISO 27799: 2008 about Health Informatics - Information Security. Management in Health using ISO / IEC 27002. Geneva: ISO.

[4] Indrajit, R.E. (2011). Information Security Standard Framework: ISO17799. Jakarta: IDSIRTII.

[5] Indonesian Government Regulation (2014). Health Information System., Jakarta: President. Republic of Indonesia.

[6] Kroll Fraud Foundation (2008). HIMSS Analytics Report: Security of Patient Data. Chicago, IL: HIMSS Analytics.

[7] Maglogiannis, Ilias. Elias Zafiropoulos (2006). "Modeling risk in is distributed healthcare information systems ", The 28th Annual International Conference of the IEEE on Engineering in Medical and Biology Society (EMBS), IEEE.

[8] Purwaningtyas, Ratri (2010). Challenges and Ethics of Information Technology. Depok: Gunadarma University.