Defensive Model for Information Systems

Majid Alshammari
School of Engineering
University of Bridgeport
United States of America

Abstract

Today, companies and government agencies relay on information systems to manage the information they have, this information may be classified, thus any disclosed by unauthorized persons may led to catastrophe consequences to those organizations. Therefore, there is urgent need for secure information systems. In this research, a defensive model for information systems is presented to address the defenses that related to these systems. The proposed defensive model is categorized into four domains: technical defense, operation defense, managerial defense, and physical defense.

Keywords: Defensive model, Information Systems, Security.

1. Introduction

Over the last decade, Information systems (IS) have been heavily used in organizations such as companies and government agencies. These systems help the organizations to mange and access the stored information. As a result, IS are considered a crucial part of these organizations given the fact most of them relay them when it comes to information processing. However, this kind of reliance may led to catastrophic consequences if any disruption occurs (Loch, Houston, & Warkentin, 1992). Fore instance, a survey of U.S. insurance companies found that 90 percent of these firms, which are dependent upon Information Systems, would fail after a significant loss or disruption of the IS facility(Carter, 1988), this survey shows that security weaknesses in IS will cause major service interruption for those companies and may unauthorized exposure of sensitive information (Ping An, 2010). Thus, it is significant to address a defensive model for the information systems to increase their security and then efficiency. In this research, a defensive model for information systems is presented to address the defenses that related to these systems.

2. Research Method

An extensive research in the existing literature of computers security, networks security, and IS helps to shape a defensive model for IS. The defensive model domain consists of four domains. First domain is technical defense. Second domain is operational defense. Third domain is managerial defense. Forth domain is physical defense. The figure below presents the four domains and the related hypothesis to reach the desired goal.

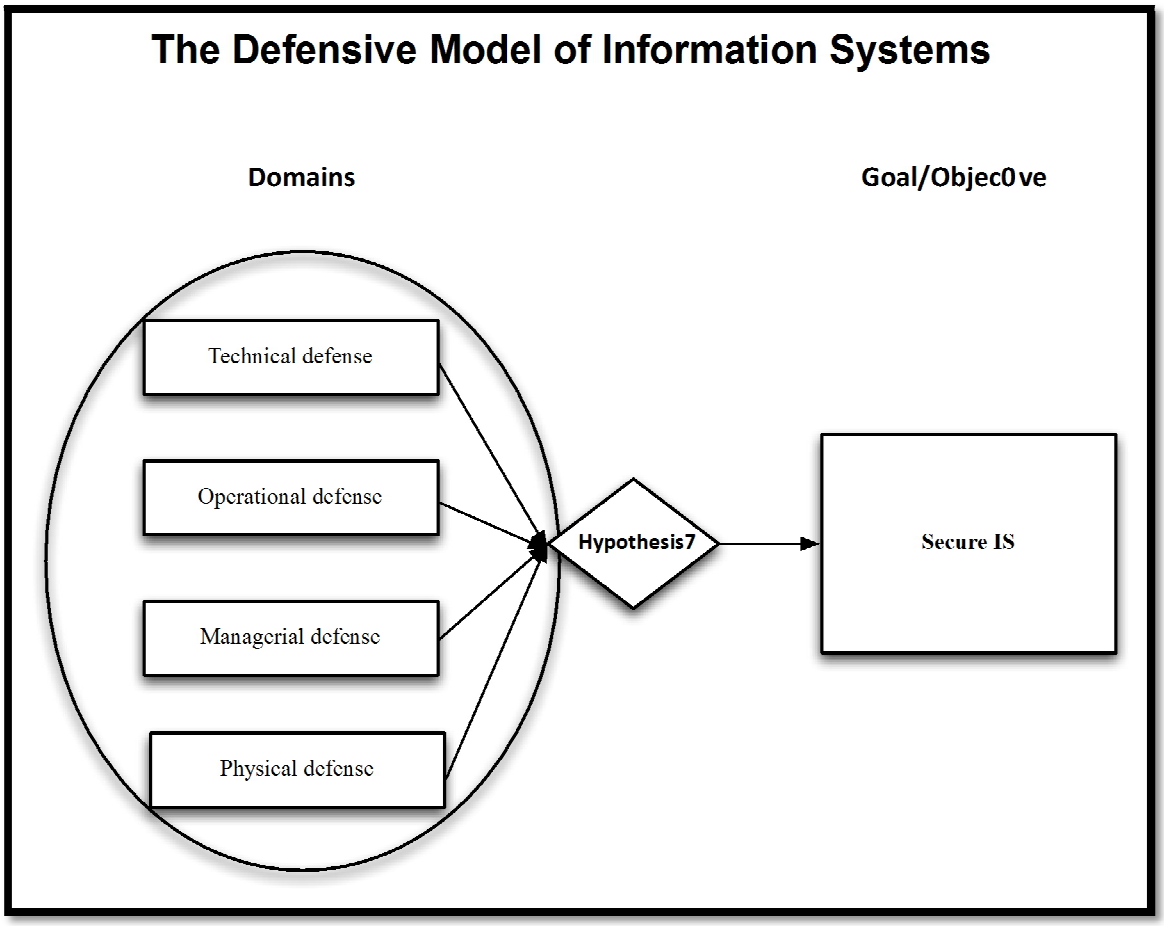

Figure 1: The defensive model.

2.1. Technical Defense

It is the first domain of the defensive model, these defenses that are used technically in computers and networks. Technical defense includes four techniques: Cryptography, Firewalls, Anti-malware, and Intrusion detection. The following describes these techniques in more detail:

Cryptography: can be implemented to achieve confidentiality, integrity, authentication, and non- repudiation (Lefton, 1991; Massey, 1986; Stallings, 2011).

Firewalls: considered first line of defense in information systems (Gouda & Liu, 2005)thus firewalls play an important role in information systems security due the fact that the Internet service is an essential to organizations because it allows employees to contact outside the word and other organization. The basic idea of firewalls is protecting information system against inside and outside intrusions.

Anti-malware: provides protection for operation systems against malicious software. Anti malware can be anti-virus, or anti-spyware. Malware can be found in files, executable programs, and the operation system(Marx, 2000). Therefore, information systems should have anti malware. Intrusion detection provides real time warnings for information systems by monitoring and analysis the any attempts to access the system.

Intrusion detection: will fire an alarm when adversaries try to exploit vulnerabilities of software for opening a backdoor into it(Zhuowei, Das, & Jianying, 2005).

2.2. Operational Defense

It is the second domain of the defensive model, Operational defense has a significant role in the management of information systems security (Haddad et al., 2011), even if organizations have applied technical security to their information systems such as encryption, firewalls, and intrusion detection, they need to set up security policies for the system to avoid humans mistakes.

Operation defenses include two approaches: policy and training. The following describes these approaches in more detail:

Policies: security policy is made up of documents that do not provide technical and implementation details. It only provides management rules for IS. Applying a secure policy to IS helps to manage the implementation of these systems (Cosic & Boban, 2010).

Training: trained employees have more security skills than other employees because they will be updated with the most new threats.

2.3 Managerial defense

It is the third domain of the defensive model, managerial defense Involves putting standards for hiring people such as preforming an extensive background check on the candidates(Bottino, 2006). The importance of background check comes from the following cases:

Hiring an adequate person: if an organization hired inadequate person to mange the IS, he or she may misuse with configuration and implementation that may lead to open holes or backdoors, as a result this person become a threat to the IS.

Hiring criminals: if an organization hired a criminal person, he or she may sell the organization information to another organization.

2.4 Physical defense

It is the forth domain of the defensive model, physical defense Involves defenses for physical assets. Physical defense is also important due that fact that physical equipment is very expansive and any damage for the equipment may cause data loss. In fact, physical defense provides protection to the IS against natural disasters, technical faults, and human. The following describes these disasters in more detail:

Natural disaster: one of the most dangerous threats to IS, for example hurricane and strong wind may cause damage to the physical equipment by flying objects. Another example, earthquake also causes damages to physical equipment. Therefore, an organization may uses off site equipment.

Technical faults: such as electrical overvoltage, electrical under voltage, and electrical interruption, all of them considered as threats to IS. There for organizations must use stand by generators.

Human: are considered unusual and unpredictable threats and they can be classified into three categories of threats: unauthorized physical access, devastation, and theft. The unauthorized physical access occurs when an unauthorized person access to restricted areas for copying data. The devastation occurs when an unauthorized person access to restricted areas for destroying IS equipment. The theft means stealing of equipment and official papers. Therefore, organizations should have restricted rules for accessing the desired places.

3. The Defensive Model and IS components.

In general, Information systems (IS) can be described as a system that consists of three major components. The first component is computers. The second component is the network. And the third component is the human. Thus, the IS defensive model should bead equate to cover all the three components. More precisely, some of the defensive model domains secure one (at least) or more of IS components. The following table shows the scope of each defensive model domain with IS components.

ISComponents	**Defense Domains**			
	Technical defense	**Operational defense**	**Managerial defense**	**Physical defense**
Computers	✔	✔		✔
Networks	✔	✔		✔
Human		✔	✔	

Figure 2: The scope of the defensive model and IS components.

4. Conclusion

Due the fact that most organizations relay on information systems, security of these systems should be a top priority for the organizations because any disruption of the system will lead to unwanted results. Therefore, applying the defensive model will help these organizations to understand the big picture of IS security. Also, the proposed defensive model covers four domains: Technical, Operational, Managerial, and Physical defense.

References

Bottino, L. J. (2006, 15-19 Oct. 2006). Security Measures in a Secure Computer Communications Architecture. Paper presented at the 25th Digital Avionics Systems Conference, 2006 IEEE/AIAA.

Carter, R. (1988). Dependence and Disaster- Recovering from EDP Systems Failur. Management Services (UK) (32:12), pp.20-22.

Cosic, Z., & Boban, M. (2010, 10-11 Sept. 2010). Information security management — Defining approaches to Information Security policies in ISMS. Paper presented at the Intelligent Systems and Informatics (SISY), 2010 8th International Symposium on.

Gouda, M. G., & Liu, A. X. (2005, 28 June-1 July 2005). A model of stateful firewalls and its properties. Paper presented at the Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on.

Haddad, S., Dubus, S., Hecker, A., Kanstren, T., Marquet, B., & Savola, R. (2011, 26-28 Sept. 2011). Operational security assurance evaluation in open infrastructures. Paper presented at the Risk and Security of Internet and Systems (CRiSIS), 2011 6th International Conference on.

Lefton, P. (1991). Number Theory and Public-Key Cryptography. The Mathematics Teacher, 84(1), 54-62. doi: 10.2307/27967000

Loch, K. D., Houston, H. C., & Warkentin, M. E. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. MIS Quarterly, 16(2), 173-186.

Marx, A. (2000). A guideline to anti-malware-software testing. European Institute for Computer Anti-Virus Research (EICAR), 218-253.

Massey, J. L. (1986). Cryptography—A selective survey. Digital Communications, 85, 3-25.

Ping An, W. (2010, 22-24 June 2010). Information security knowledge and behavior: An adapted model of technology acceptance. Paper presented at the Education Technology and Computer (ICETC), 2010 2nd International Conference on.

Stallings, W. (2011). Cryptography and Network Security, 5/E: Pearson Education NY.

Zhuowei, L., Das, A., & Jianying, Z. (2005, 15-17 June 2005). Theoretical basis for intrusion detection. Paper presented at the Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC.