DEFENSE MECHANISMS FOR COMPUTER-BASED INFORMATION SYSTEMS

Majid Alshammari[1] and Christian Bach[2]

[1] Department of Computer Science and Engineering, School of Engineering, University of Bridgeport

[2] Department of Technology Management and Biomedical Engineering, School of Engineering, University of Bridgeport

ABSTRACT

Nowadays, corporations and a government agencies relay on computer-based information system to manage their information, this information may be classified, so it will be dangerous if it is disclosed by unauthorized persons. Therefore, there is urgent need for defense. In this research, defense has been categorized into four mechanisms technical defense, operation defense, management defense, and physical defense based on the logic of computer and network security. Also, each mechanism has been investigated and explained in the term of computer based information systems.

KEYWARDS

ComputerBased Information System,

INTRODUCTION

Computer-based information systems CBIS have been around for a long time in organization. These systems help organizations to get a reliable and a centralized access to their stored information. Accordingly, most of organizations relay on computer based information systems, but this kind of reliance may be catastrophic if a disruption occurs [1]. An example, a survey of U.S. insurance companies found that 90 percent of these firms, which are dependent upon computer based information systems, would fail after a significant loss or disruption of the CBIS facility [2], this survey shows the importance of computer based information systems security because any security weakness in computer based information systems may led to major service interruption, and may unwanted exposure of sensitive information of the organizations [3]. Thus, it is importance to investigate the defense mechanisms for computer-based information systems to increase its efficiency and security.

DOI : 10.5121/ijnsa.2013.5509

Computer-based information systems have three major components. The first component is computers. The second component is network. And the third component is human. Therefore, Implementation defense mechanisms for computer-based information systems should cover all the three components.

RESEARCH METHOD

An extensive literature search in computers security, networks security, and computer-based information systems helps to build a general model for defense mechanisms of computer-based information system. The first mechanism is technical defense. The second mechanism is operational defense. The third mechanism is managerial defense. The forth mechanism is physical defense. The figure below presents the four mechanisms and the related hypothesis to reach the desired goal.

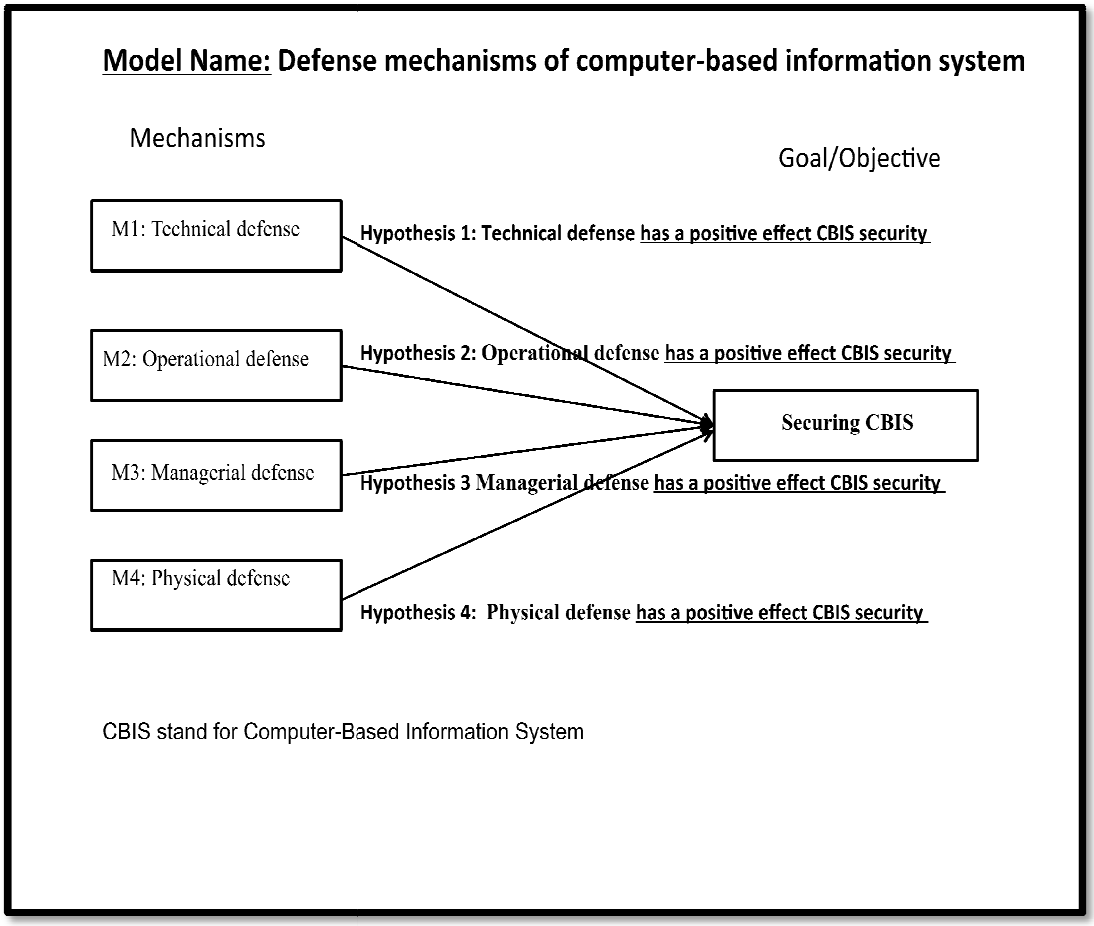

Figure 1: Defense mechanism model of computer-based information system

M1: TECHNICAL DEFENSE

Technical defense involves defenses that are used in computers and networks technically. Technical defense can be encryption, firewall, antimalware, and intrusion detection.

Encryption provides confidentiality for information exchange. The basic idea of encryption is transferring the plain text into cipher text to hide the information from unauthorized person. Therefore, Encryption is considered as technical defenses that make the information exchange invisible for an attacker. If the organization has firewalls, anti viruses, anti spyware, and strong security policies information exchange is not secured simply the information is exchanged in plan text. [4] Therefore, encryption provides confidentiality. There are two types of Encryption. The first type is symmetric encryption, known as conventional encryption, or single-key encryption involves using one key between the communicating parties. When two entities or parties want to communicate they should first agree on using one key then using this key for encryption and decryption. Symmetric encryption relays on the secrecy of the key, so keeping is important because if an opponent gained this key he/she will compromise the system. The second type of encryption is asymmetric encryption, involves using two different keys one is a public key and the other one is a private key. When two entities or parties want to communicate they should first exchange their public key and keep their private keys secure. For example, when an entity A want to communicate securely with another entity B, it encrypt a message with B's public key then send it B, B decrypt the message with its private key. There are many software and hardware in the market that support both of symmetric encryption and asymmetric encryption. Organizations should use encryption to provide data confidentiality.

Firewalls are necessary of securing the computer information system. Today the Internet service is necessary to the organizations; it allows employees of an organization network to contact to the outside word, so there is need for first line defense. Firewalls consider as first line defense for computer information systems [5]. The basic idea of firewalls is protecting information system against outside and inside attacks, so the working by filtering incoming packet and outgoing packet. Generally, most firewalls have two default policies. The first one is discard; means if an arriving packet dose not matches any rule in IPtable discard it. The second one is allow; means an arriving packet dose not match any rule in IPtable allow it to pass. Moreover, there are two types of firewalls, packet-based firewall and Stateful-based firewall. Packet – based firewall also called Packet filtering, it works by inspecting or checking the IP filed of each packet then it take a decision whether it allow the packet to pass or deny it based on the IP address of the source, the IP address of the destination, the source port number whether it TCP or UDP and the destination port [6] This type of firewalls relays on IPtable, the IPtable is set of rules that have been set by network administrator. For example, the network administrator may set a rule deny any packet comes form 192.168.1.10 with port number 80. When this packet arrives to the firewall, it will check the IPtable to take the decision. Packet firewall is easy to install, and complex to mange because you need to set many rules. Statefull firewall provides more advance future by keeping track of a given connection; it works in transport layer and the application layers. Statefullfirewall inspects a packet like the packet firewall, but it tracks the TCP connection. When a packet arrive it checks the packet filed, if the packet matched the passing policy, it add it as an entity to the IPtable and keep track for the TCP sequence to protect the session from attacks. There are numerous of software and hardware firewalls in market today, and as the treats growing up the security companies will never stop developing security tools. Firewalls one of the most impotent tools. It is worth to mention that firewall can be a feature that is added to operation system, router, and access points. For example, most operating systems OS have built-in firewall, but users may activate it.

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 [7]. Therefore, computer information systems should have anti malware.

Intrusion detection provides real time warnings for computer information system by monitoring and analysis the any attempts to access the system. Intrusion detection will fire an alarm when attackers try to exploit vulnerabilities of software for opening a backdoor into it [8]. Generally, Intrusion Detection can be classified into Host-based intrusion detection and Network-based intrusion detection. Host-based Intrusion Detection adds an extra layer of security for a host. It uses the operating system OS information to determine attacks [9] such as user logs, and software activity. Network-based intrusion detection (NID) is monitoring the network traffic at some place on a network. It checks each packet to detect illegitimate traffic. NID can monitors network and transport layers activity. Usually NID have sensors and one or more servers for in one network, the sensors are used to monitor traffic on different location in the network, and the servers are used to manage the sensors [10]. Generally, there are two techniques for intrusion detection, anomaly detection and signature detection. Anomaly detection is gathering information related to the behavior of users then analysis it to determine whether the behavior is legitimate or not [11] The second approach is signature detection, it attempts to set rules or attack patterns to determine whether it is legitimate or not. Therefore, computer information systems should have one or more Intrusion detection.

M2: OPERATIONAL DEFENSE

Operational defense has a significant role in the management of computer information systems security [12]. Therefore, even if organizations have applied technical security to their computer information system such as encryption, firewalls, and intrusion detection, they need to set up security policies for the system. Usually, operation defenses include two approaches. The first approach is setting up security policies for computer information system. The security policy has important role in term of information security management for computer information system implementation. [13] Security policy is made up of documents that do not provide technical and implementation details. It only provides management rules for computer information system. The second approach is personnel training for the employee.

M3: MANAGERIAL DEFENSE

Involves putting standards for hiring people. For example, an extensive background check and an extensive security background check [14] The importance of background check come from the following example, if an organization hire inadequate person to mange the computer information system, he or she may misuse with configuration and implementation that may lead to open holes or backdoors in CBIS as a result this person become a threat to the system. Also, security background check is very impotent because if an organization hires a criminal person, he or she may sell the organization information to another organization.

M4: PHYSICAL DEFENSE

Involves defenses for physical assets. Physical defense is important for two reasons. First reason, physical equipment is very expansive. The second reason, any damage for the equipment may cause data loss. Also, physical defense provides protection to the computer information systems against Natural disasters, technical faults, andhuman. Natural disaster one of the most dangerous threats to computer information system, for example hurricane may cause damage to the physical

equipment by strong wind and flying objects. Another example, earthquake also cause damages to physical equipment. Therefore, an organization may uses off site equipment. Technical faults such as electrical overvoltage, electrical under-voltage, and electrical interruption are considered as threats to computer information system. Electrical under-voltage takes place when computer information systems receive less voltage than they need to work normally. Electrical overvoltage occurs when computer information systems receive high voltage than they need to work. Therefor an organization may use stand by generators. Human cause unusual and unpredictable threats to computer information systems. Human threat can be classified into three categories; unauthorized physical access, theft, and misuse. The first category is unauthorized physical access, it occurs when an unauthorized person access to restricted areas for copying data, or misuse. The second category is thefts, which means theft of equipment and official papers. Therefore, the organization should have restricted rules for accessing the desired places.

RELATIONSHIP BETWEENDEFENSE MECHANISM MODEL AND CBIS COMPONENTS

Computer-based information systems have three major components, computers, network, and human. Thus, based on the model each component must be secured by at least one of the defense mechanisms. The table below presents the relationship.

CBIS components	Defense Mechanisms			
	Technical defense	Operational defense	Managerial defense	Physical defense
Computers	□	□		□
Networks	□	□		□
Human		□	□	

Table 2: The relationship between defense mechanism and CBIS components

CONCLUSION

Security of computer-based information system should be a top priority for organizations because a disruption of the CBIS will lead to unwanted results. Thus, organizations should implement the defense mechanisms to protect their information. The first mechanism (Technical defense) provides defense to the system by using software and hardware, for example, encryption, firewall, anti-malware, and intrusion detection. The second mechanism (Operational defense) provides defense to the system by setting up system policies. The third mechanism (Managerial defense) provides defense to the system by putting standard for hiring. The forth mechanism (Physical defense) provides defense to physical assets**.**

REFERENCES

[1] K. D. Loch, H. C. Houston, and M. E. Warkentin, "Threats to Information Systems: Today's Reality, Yesterday's Understanding," MIS Quarterly, vol. 16, pp. 173-186, 1992.

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

[3] W. Ping An, "Information security knowledge and behavior: An adapted model of technology acceptance," in Education Technology and Computer (ICETC), 2010 2nd International Conference on, 2010, pp. V2-364-V2-367.

[4] H. Li and P. ZhaoJian, "Security Research on P2P Network," in Computational Intelligence and Software Engineering, 2009. CiSE 2009. International Conference on, 2009, pp. 1-5.

[5] M. G. Gouda and A. X. Liu, "A model of stateful firewalls and its properties," in Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on, 2005, pp. 128-137.

[6] Y. Xin, C. Wei, and W. Yantao, "The research of firewall technology in computer network security," in Computational Intelligence and Industrial Applications, 2009. PACIIA 2009. Asia-Pacific Conference on, 2009, pp. 421-424.

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

[8] L. Zhuowei, A. Das, and Z. Jianying, "Theoretical basis for intrusion detection," in Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC, 2005, pp. 184-192.

[9] Y. Lin, Y. Zhang, and Y.-j. Ou, "The Design and Implementation of Host-Based Intrusion Detection System," in Intelligent Information Technology and Security Informatics (IITSI), 2010 Third International Symposium on, 2010, pp. 595-598.

[10] B. Mukherjee, L. T. Heberlein, and K. N. Levitt, "Network intrusion detection," Network, IEEE, vol. 8, pp. 26-41, 1994.

[11] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Computing Surveys (CSUR), vol. 41, p. 15, 2009.

[12] S. Haddad, S. Dubus, A. Hecker, T. Kanstren, B. Marquet, and R. Savola, "Operational security assurance evaluation in open infrastructures," in Risk and Security of Internet and Systems (CRiSIS), 2011 6th International Conference on, 2011, pp. 1-6.

[13] Z. Cosic and M. Boban, "Information security management — Defining approaches to Information Security policies in ISMS," in Intelligent Systems and Informatics (SISY), 2010 8th International Symposium on, 2010, pp. 83-85.

[14] L. J. Bottino, "Security Measures in a Secure Computer Communications Architecture," in 25th Digital Avionics Systems Conference, 2006 IEEE/AIAA, 2006, pp. 1-18.

AUTHORS

Majid Alshammari

Majid Alshammari received his MS in computer science and Graduate Certificate in Information Protection and Security from University of New Have at West Haven, Connecticut, USA. He is pursuing his Doctorate in Computer Science and Engineering at the University of Bridgeport at Bridgeport, Connecticut, USA. He is MCSEs and CEH. His research interests include network, computer and information security. He is a member of the Association for Computer society and information society, IEEE.

Christian Bach

Christian Bach is an Assistant Professor of Technology Management and Biomedical Engineering at University of Bridgeport. He received his MBA and PhD in Information Science from University at Albany SUNY in Albany, New York. Some of Dr. Bach's research interests include Intracellular Immunization, induced Pluripotent Stem (iPS) cells, Artificial Transcription Factors, Target Detection Assay, Microarr ays, Bioreactors, Protein Folding (micro -level), Target Binding Site Computation, micro Database Systems, and Knowledge Cubes. He is the author of multiple journal articles including "Tower Computing: Utilization of Cloud Computing in science-based Knet environments," "Employing the Intellectual Bandwidth Model for Measuring Value Creation in Collaborative Environments," and "Scientific and Philosophical Aspects of Information and the Relationships among Data, Information, and Knowledge."