SADI International Journal of Science, Engineering and Technology
ISSN: 2837-1941| Impact Factor: 8.27
Volume. 12, Number 3; July - September, 2025;
Published By: Scientific and Academic Development Institute (SADI)
8933 Willis AveLos Angeles, California
https://sadijournals.org/index.php/sijset|editorial@sadijournals.org

TECHNIQUES FOR SECURING COMPUTER-BASED INFORMATION SYSTEMS

D. O. Egete [1] and B. I. Ele[2]
[1, 2]Department of Computer Science, University of Calabar, Calabar, Nigeria
Emails: mydays2020@gmail.com / davidoboboho@gmail.com,
Phone: +234(0)8064451381 / +234(0)8037204626
DOI: https://doi.org/10.5281/zenodo.16894975

Abstract: Nowadays, corporations and government agencies rely on computer-based information systems to manage their information. This information may be classified, so it will be dangerous if it is disclosed by unauthorized persons. Therefore, there is an urgent need for defense. In this research, defense has been categorized into four mechanisms based on the logic of computer and network security: technical defense, operational defense, management defense, and physical defense. Each mechanism has been investigated and explained with respect to computer-based information systems.

Keywords: Computer-Based Information System, Defense Mechanism Model, Technical Defense, Physical Defense, Operational Defense, Management Defense

1. INTRODUCTION

CBIS have been around for a long time in organizations. These systems help organizations obtain reliable and centralized access to their stored information. Accordingly, most organizations rely on computer-based information systems; however, this kind of reliance may be catastrophic if a disruption occurs [1]. For example, a survey of U.S. insurance companies found that 90% of these firms, which are dependent on computer-based information systems (CBIS), would fail after a significant loss or disruption of the CBIS facility [2]. This survey shows the importance of CBIS security because any security weakness in CBIS may lead to major service interruption and may lead to unwanted exposure of sensitive information of the organizations [3]. Thus, investigating the defense mechanisms for computer-based information systems to increase their efficiency and security is important.

Computer-based information systems have three major components: The first component is computers. The second component is the network. The third component is human [18]. Therefore, implementation of defense mechanisms for the three computer components is essential.

2. RESEARCH METHODOLOGY

An extensive literature search in computer security, network security, and computer information systems helps build a general model for defense mechanisms of computer information systems. The first mechanism is technical defense. The second mechanism is the operational defense. The third mechanism is managerial defense. The

fourth mechanism is physical defense. The figure below presents the four mechanisms and the related hypotheses for achieving the desired goal.

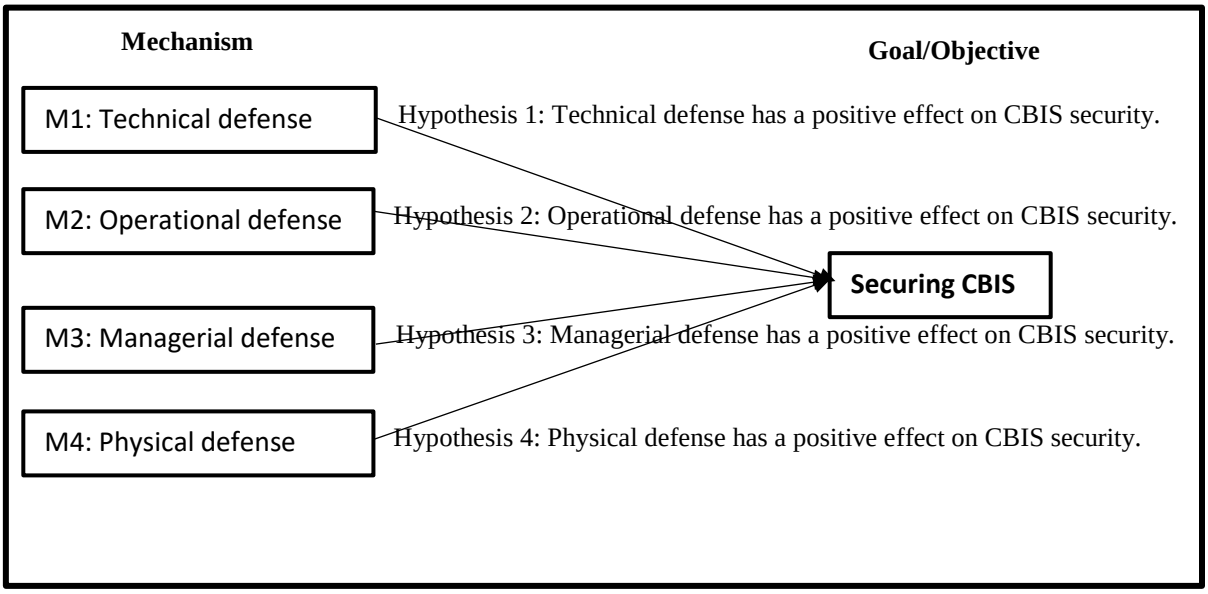

Figure 1: Defense mechanism model of a computer-based information system (CBSI)

M1: TECHNICAL DEFENSE

Technical defense involves defenses that are technically used in computers and networks.

Technical defenses include encryption, firewall, antimalware, and intrusion detection. Encryption ensures confidentiality for information exchange. The basic idea of encryption is to transfer plain text into cipher text to hide information from unauthorized persons. Therefore, encryption is considered a technical defense that makes the information exchange invisible to an attacker. If the organization has firewalls, anti-viruses, anti-spyware, and strong security policies, information exchange is not secured simply because the information is exchanged in plain 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, which involves using one key between the communicating parties [17]. When two entities or parties want to communicate, they should first agree on using one key and then using this key for encryption and decryption. Symmetric encryption relies on the secrecy of the key, so keeping this key is important because if an opponent gains this key, he/she will compromise the system. The second type of encryption is asymmetric encryption, which involves using two different keys: a public key and 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 entity A wants to communicate securely with another entity B, it encrypts a message with B's public key and then sends it to B. B decrypts the message with its private key. There are many software and hardware in the market that support both symmetric and asymmetric encryption. Organizations should use encryption to ensure data confidentiality.

Firewalls are necessary to secure the computer information system. Today, the Internet service is necessary to organizations; it allows employees of an organization network to contact the outside world, so there is a need for first-line defense. Firewalls are considered first-line defenses for computer information systems [5]. The basic idea behind firewalls is to protect an information system against outside and inside attacks, so they work by

filtering incoming and outgoing packets. Generally, most firewalls have two default policies [17]. The first one is discard, which means that if an arriving packet does not match any rule in IPtable, it is discarded. The second one is allow, which means that an arriving packet does not match any rule in the IPtable that allows it to pass. Moreover, there are two types of firewalls: packet-based and stateful-based. Packet – based firewall, also called packet filtering, works by inspecting or checking the IP field of each packet. Then, it decides whether to allow or deny the packet to pass based on the IP address of the source, the IP address of the destination, the source port number (TCP or UDP), and the destination port [6]. This type of firewall relays on the IPtable, which is a set of rules set by the network administrator. For example, the network administrator may set a rule to deny any packet that comes from 192.168.1.10 with port number 80. When this packet arrives at the firewall, it will check the IPtable to make a decision. A packet firewall is easy to install and complex to manage because many rules must be set. A stateful firewall provides a more advanced future by keeping track of a given connection; it works in the transport and application layers. A stateful firewall inspects a packet like a packet firewall, but it tracks the TCP connection. When a packet arrives, it checks the packet file. If the packet matches the passing policy, it adds it as an entity to the IPtable and keeps track of the TCP sequence to protect the session from attacks. There are numerous software and hardware firewalls in the market today, and security companies will never stop developing security tools as they grow. A firewall is one of the most important tools. It is worth mentioning that a firewall can be a feature that is added to the operating system, router, and access points. For example, most OSs have a built-in firewall, but users may activate it.

Anti-malware provides protection against malicious software for operating systems. Anti-malware can be anti-virus or anti-spyware. Malware can be found in files, executable programs, and the operating system [7]. Therefore, computer information systems should be anti-malware.

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

M2: OPERATIONAL DEFENSE

Operational defense plays a significant role in the security management of computer information systems [12]. Therefore, even if organizations have applied technical security measures such as encryption, firewalls, and intrusion detection to their computer information systems, they must set up security policies for the system. Operation defenses usually include two approaches. The first approach is to set up security policies for the computer information system. The security policy plays an important role in terms of information security management for the implementation of computer information systems. [13] A security policy is made up of

documents that do not provide technical and implementation details. It only provides management rules for the computer information system. The second approach is personnel training for the employee.

M3: MANAGERIAL DEFENSE

It involves setting standards for hiring people. For example, an extensive background check and an extensive security background check [14] can be used. The importance of a background check comes from the following example. If an organization hires an inadequate person to manage the computer information system, he or she may misuse the configuration and implementation that may lead to open holes or backdoors in the CBIS. As a result, this person becomes a threat to the system. Also, a security background check is very impotent because if an organization hires a criminal, he or she may sell the organization's information to another organization.

M4: PHYSICAL DEFENSE

It involves defenses for physical assets. Physical defense is important for two reasons. First, physical equipment is very expansive. Second, any damage to the equipment may cause data loss. Physical defense provides protection to computer information systems against natural disasters, technical faults, and human error [16]. Natural disasters are one of the most dangerous threats to computer information systems. For example, hurricanes may cause damage to physical equipment by strong winds and flying objects. Another example of an earthquake that causes damage to physical equipment. Therefore, an organization may use off-site equipment. Technical faults, such as electrical overvoltage, electrical undervoltage, and electrical interruption, are considered threats to the computer information system. Electrical undervoltage occurs when computer information systems receive less voltage than they need to work normally. Electrical overvoltage occurs when a computer information system receives a higher voltage than it needs to work. Therefore, an organization may use stand-by generators. Humans cause unusual and unpredictable threats to computer information systems. Human threats can be classified into three categories: unauthorized physical access, theft, and misuse [19]. The first category is unauthorized physical access, which occurs when an unauthorized person accesses restricted areas for copying data or misuses them. The second category is thefts, i.e., theft of equipment and official papers. Therefore, the organization should have restricted access to the desired places.

3. RELATIONSHIP BETWEEN DEFENSE MECHANISM MODEL AND COMPUTER-BASED INFORMATION SYSTEM COMPONENTS

Computer-based information systems have three major components: computers, networks, and humans. Thus, each component must be secured by at least one of the defense mechanisms based on the model. Table 2 below presents the relationship.

CBIS COMPONENTS	DEFENSE MECHANISMS			
	Technical defense	**Operational defense**	**Managerial defense**	**Physical defense**
COMPUTERS	Yes	Yes	No	Yes
NETWORKS	Yes	Yes	No	Yes
HUMAN	No	Yes	Yes	No

Table 2: Relationship between the defense mechanism and CBIS components

4. CONCLUSION

The security of CBIS should be a top priority for organizations because a disruption of the CBIS will lead to unwanted results. Therefore, organizations should implement defense mechanisms to protect their information. The first mechanism (technical defense) provides defense to the system 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 setting the hiring standard. The fourth mechanism (physical defense) provides defense to physical assets**.**

REFERENCES

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.

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

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.

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.

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.

Y. Xin, C. Wei, and W. Yantao, "The research of firewall technology in computer network security," in Computational Intelligence and Industrial Applications, 2009. p. 109. PACIIA 2009. Asia-Pacific Conference on, 2009, pp. 421-424.

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

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, 2005.

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.

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

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

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.

Z. CosmiC 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.

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

M. Alshammari and C. Bach, "Defense Mechanisms for Computer-Based Information Systems". International Journal of Network Security & Its Applications (IJNSA), 2013, 5(5), pp. 37-48.

B. I. Ele, M. A. Agana and P. T. Bukie, "A Distributed Airline Reservation System for Nigerian Airline Companies". COMPUSOFT, An international journal of advanced computer technology, 7(6), 2018.

B. I. Ele, "An Enhanced Mechanism for Protecting Web Applications from Cross Site Request Forgery (CSRF)". British Journal of Computer, Networking and Information Technology 6(1), 1-17, 2024. DOI: 10.52589/BJCNIT-R5YYKXKA.

B. I. Ele, A. O. Ofem, P. T. Bukie and J. O. Esin, "Adopting Effective Computer Maintenance and Troubleshooting Culture for Sustainable Development of IT-Driven Sectors of the Third World Countries". The Journal of Educational Research and Technology (JERT), 5(5), 2018.

D. O. Egete, B. I. Ele, E. E. Umoh and D. U. Ashishie, "A model of an improved fault-tolerant system for wireless network". International Journal of Natural and Applied Sciences (IJNAS), VOL. 12, Special Edition (2019); P. 141 – 144, 2019.