ClinicSearch

International Journal of Clinical Epidemiology

Cheryl Ann Alexander *

Open Access

Review Article

Designing a Cybersecurity Awareness and Training Program for a Large Medical Center

Cheryl Ann Alexander [1]* and Lidong Wang [2]

[1]Institute for IT Innovation and Smart Health, Mississippi, USA.

[2]Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA.

***Correspondence Author:** Cheryl Ann Alexander, Institute for IT Innovation and Smart Health, Mississippi, USA

Received Date: March 08, 2024 | Accepted Date: March 15, 2024| Published Date: March 20, 2024

Citation: Cheryl A. Alexande rand Lidong Wang, (2024), Designing a Cybersecurity Awareness and Training Program for a Large Medical Center, *International Journal of Clinical Epidemiology*, 3(2); **DOI:**10.31579/2835-9232/056

Abstract

This review paper investigates Open Systems Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) are networking models that support interoperability and reduce proprietary incompatibilities. This paper investigates whether Internet Protocol (IP) data transmissions are vulnerable to being interrupted and modified. Attack vectors at the network level also include man-in-the-middle attack, spoofing or forging of a network address, denial of service (DoS), etc. User Datagram Protocol (UDP) and TCP are transport layer protocols. Attack vectors in the transport layer are attacks using UDP (considered unreliable) and TCP, for example, SYN flood attacks. The session layer and the presentation layer are not popular targets for common attacks. The protocols of the application layer include File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), etc. The centralized program management model (Wilson and Hash, 2003) is used. However, in this model, a centralized policy, strategy, and implementation are used while Charleston Regional Medical Center in the US does not spread over a wide geographical area, it has a centralized structure. The information systems security manager is the Chief Information Officer (CIO) in the center. TCP/IP is also an example of a multilayer protocol. Attackers can also use multilayer protocol encapsulation to secure the capacity to fool interior switching devices to achieve entrance to a virtual local area network (VLAN).

Keywords: open systems interconnection (osi); transmission control protocol (tcp); internet protocol (ip); attack vector;training program; cybersecurity

Introduction

Networking models support interoperability and reduce proprietary incompatibilities. Two prevailing models are Open Systems Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP). Figure 1 shows the two models. There are seven layers in the OSI model, while there are four layers in the TCP/IP model (also called DARPA model) (Warsinske et al., 2019).

TCP/IP Model	OSI Model
Application	Application
	Presentation
	Session
Transport	Transport
Internet	Network
Link	Data Link
	Physical

Figure 1: OSI and TCP/IP Models

Internet Protocol (IP) data transmissions are susceptible to being intercepted and altered. Attack vectors in the network layer include man-in-the-middle attacks, spoofing or forging of a network address, denial of service (DoS), etc. User Datagram Protocol (UDP) and TCP are transport layer protocols. Attack vectors in the transport layer include attacks using UDP (considered unreliable) and TCP, for example, SYN flood attacks. The session layer and the presentation layer aren't popular targets for common attacks. The protocols of the application layer include File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), etc. Attack vectors in the application layer include SQL injection or cross-site scripting, HTTP-based attacks such as an HTTP flood or input validation attacks, etc. TCP/IP is also an example of a multilayer protocol. Attackers

can also use multilayer protocol encapsulation to provide an ability to fool interior switching devices to gain access to a virtual local area network (VLAN) (Warsinske et al., 2019).

The purpose of the work is to design a security awareness and training program so that employees in Charleston Regional Medical Center (a large medical center in the US) understand their security responsibilities, information security risks related to their activities, and policies in the center.

2. Audiences, Roles, and Responsibilities

Audiences of the program in the Medical Center include four target groups. Group 1 includes providers (i.e., physicians, nurse practitioners, physician assistants), nurses, pharmacists, techs, and staff (e.g., certified nursing assistants (CNAs), techs, clerks, etc.). Group 2 includes Stakeholders (i.e., ambulance personnel, transferring staff members, secondary hospital staff such as providers and nurses, delivery personnel, etc.), security personnel, external delivery personnel, etc. Group 3 includes the CEO, financial staff, Chief Nursing Officer, and department heads (other than the information systems security manager). Group 4 includes the information systems security manager and other IT staff, data analytics staff, etc., in the information systems security department. The CEO assigns responsibility to the information systems security manager for the security training and the security program implementation. The information systems security manager directs other information systems security department members, ensures the members with substantial security responsibilities, ensures the training with quality implementation, and ensures effective tracking and reporting mechanisms. The information systems security department members assist other employees in the Medical Center in completing training and help them fix problems in information systems security.

Other employees can be called users of information systems or resources. They are the largest audience in the center. They need to understand and observe security policies and procedures in the center, complete training on time, and keep software updated with security patches. Their activities for security include data backup, suitable password use, appropriate antivirus protection, etc.

3. Components of the Program: Awareness, Training, and Education

Learning starts with awareness, goes to training, and progresses to education. Awareness is to focus attention on security. Training endeavors to obtain security skills and competencies. Education helps to achieve knowledge and produce security specialists and professionals (Wilson and Hash, 2003).

Professional development validates skills through certification. There are two kinds of certification: technical and general. The general focus is on a foundation of knowledge. The technical focus is on technical security (Wilson and Hash, 2003). Data analytics, AI, blockchain, and their applications in cybersecurity are very useful topics for professional development.

4. Designing an Awareness and Training Program

4.1 Structuring an awareness and training program

The centralized program management model (Wilson and Hash, 2003) is used. The model is centralized policy, strategy, and implementation. The Medical Center does not spread over a wide geographical area; it has a centralized structure. Figure 2 shows the model implemented in the Medical Center. The information systems security manager is the Chief Information Officer (CIO) in the center.

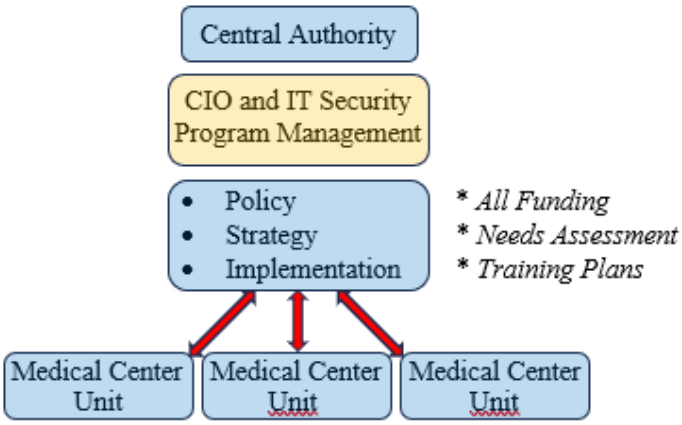

Figure 2. Centralized Program Management

4.2 Developing an awareness and training plan

All employees in the four target groups need to complete universal training annually. The training includes 1) computers being covered with privacy screens, 2) not chatting about patients in the elevator and other public places, 3) regulations for Centers for Medicare & Medicaid Services (CMS) and Medicaid, 4) not reading information from charts if you aren't taking care of the patient, 5) biometric screening, barcodes for medication safety. The following are training for specific target groups.

Role 1*: *Group 1 (including providers, nurses, pharmacists, techs, and staff)

Learning Objectives: Learn enough security knowledge of patient data, treat patients, provide medications, and provide patient care while protecting patient data from malicious actors.

Focus Areas: They need training in the use of barcodes, the Health Insurance Portability and Accountability Act (HIPAA), biometrics (e.g., fingerprint, iris scanning, and facial recognition), and security regulations.

Providers, nurses, and all bedside staff need additional training on ICD-10 billing requirements, security requirements for data protection, and regulatory standards.

Methods/Activities:

Both online training and physical showing in the training rooms are acceptable; physical showing in the training rooms is recommended for employees with a weak background in IT and computer application knowledge.

Schedule:

An annual training of two hours is scheduled.

***Evaluation Criteria*:**

A test is performed right after the training. An individual will get a certificate after getting a grade of 80%. Everyone can try the training and test four times.

Role 2: Group 2 (including stakeholders, security personnel, external delivery personnel, etc.)

Learning Objectives: Learn how to protect patient data physically with the aid of screen protectors and biometrics, and how to identify malicious actors.

Focus Areas:

Regulatory standards, HIPAA, and biometrics

Methods/Activities: Both online training and physical showing in the training rooms are acceptable. Physical showing in the training rooms is recommended for employees with a weak background in IT and computer application knowledge.

Schedule:

An annual training of two hours is scheduled.

Evaluation Criteria: A test is performed right after the training. An individual will get a certificate after getting a grade of 80%. Everyone can try the training and test four times.

Role 3: Group 3 (including CEO, financial staff, Chief Nursing Officer, and department heads)

Learning Objectives: Receive enough knowledge to protect patient data, protect the financial status of the facility, and learn how to protect each department from malicious actors.

Focus Areas: Regulatory standards, biometrics, HIPAA, and data security.

Methods/Activities: Both online training and physical showing in the training rooms are acceptable; physical showing in the training rooms is recommended for employees with a weak background in IT and computer application knowledge.

Schedule: An annual training of two hours is scheduled.

Evaluation Criteria: A test is performed right after the training. An individual will get a certificate after getting a grade of 80%. Everyone can try the training and test four times.

Role 4: Group 4, including the information systems security manager and other IT staff, data analytics staff, etc., in the information systems security department.

Learning Objectives: Have enough deep knowledge to provide security services within the hospital and professional skills to control data.

Focus Areas: Compatibility among applications, validating the integrity of applications before installation, configuring firewalls, monitoring network activity, intrusion detection systems (IDS), managing network bridges and routers, managing account privileges, auditing account activity, security for all hospital departments, etc.

Schedule: An annual training of two hours is scheduled.

Evaluation Criteria: A test is performed right after the training. An individual will get a certificate after getting a grade of 80%. Everyone can try the training and test three times.

4.3 Developing Awareness and Training Materials

Awareness topics can be selected as follows (Wilson and Hash, 2003):

1) Unknown e-mail and attachments

2) Social engineering

3) Laptop security while on travel – address both physical and information security issues

4) Desktop security

5) Protect information subject to confidentiality concerns

Sources of awareness material (Wilson and Hash, 2003) can be:

1) Online IT security websites

2) Professional journals

3) Conferences and courses.

A Model for Building Training Courses: NIST Special Pub. 800-16 (Wilson and Hash, 2003) is recommended as training material.

5. Conclusion

In this paper, Open Systems Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) are networking models that support interoperability and decrease proprietary mismatches. This paper investigates whether Internet Protocol (IP) data transmissions are vulnerable to being interrupted and modified. Attack vectors at the network level also include man-in-the-middle attack, spoofing or forging of a network address, denial of service (DoS), etc. User Datagram Protocol (UDP) and TCP are transport layer protocols. Attack vectors in the transport layer are attacks using UDP (considered unreliable) and TCP, for example, SYN flood attacks. The session layer and the presentation layer are not popular targets for common attacks. The protocols of the application layer include File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), etc. The centralized program management model (Wilson and Hash, 2003) is used. However, in this model, a centralized policy, strategy, and implementation are used and while the Medical Center does not spread over a wide geographical area, it has a centralized structure. The information systems security manager is the Chief Information Officer (CIO) in the center. TCP/IP is also an example of a multilayer protocol. Attackers can also use multilayer protocol encapsulation to secure the capacity to fool interior switching devices to achieve entrance to a virtual local area network (VLAN).

In a healthcare center, the protection of patient data has become a crucial step in providing care to patients. For providers, nurses, staff, and non-licensed personnel, the need to be educated on protecting patient care is essential to keeping data safe from malicious actors. A substantial educational program is necessary for staff to understand cybersecurity in the healthcare setting, and to ensure the correct steps for learning how to protect patient data. The model for building a better training program lies in the Model for Building Training Courses. Within the document, many uses of the tool can be modified for the development of a strong educational program for protecting patient data and educating staff, providers, IT staff, etc.

Acknowledgements

The authors would like to express thanks to Technology and Healthcare Solutions, USA for its help and support.

Conflict of interest

The authors would like to announce that there is no conflict of interest.

References

1. Warsinske, J., Henry, K., Graff, M., Hoover, C., Malisow, B., Murphy, S., ... & Vasquez, M. (2019). *The Official (ISC) 2 Guide to the CISSP CBK Reference*. John Wiley & Sons.
2. Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special publication*, *800*(50), 31-39.