AUCTORES
Globalize your Research

Journal of General Medicine and Clinical Practice
Cheryl Ann Alexander *

Open Access

Research Article

Asset Security and Asset Management: Cybersecurity Case Study of 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.

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

Received date: April 15, 2024; **Accepted date:** May 09, 2024; **Published date:** May 15, 2024

Citation: Cheryl A. Alexander and Lidong Wang, (2024), Asset Security and Asset Management: Cybersecurity Case Study of a Large Medical Center, *J. General Medicine and Clinical Practice,* 7(9); **DOI:**10.31579/2639-4162/176

Abstract

Asset management is a crucial process for every enterprise. Asset classification is necessary to determine the risk factors for cybercrimes and the safety of essential equipment, medications, hardware and software, and data. Identification of information and classifying data and the associated equipment can alleviate surprise attacks and prevent criminals from absconding with data or other data-related equipment. There are numerous levels of classification, and it is critical to look at vulnerabilities and what information or data needs the most protection. Data policy, data governance, and data standards protect data and should be considered when classifying the data. This paper discusses developing an asset security and management program for a mid-level medical center. Data is an essential asset in any medical center and the identification of hardware and software components and application patch levels that can be categorized are key elements of cybersecurity.

Kew Words: cybersecurity; data governance; data policy; asset management; asset classifications

Introduction

Information management across industries has significantly changed as critical blind spots have become increasingly more difficult to find and repair for professionals, and tools for protecting data have failed to meet the challenges of defending that data. As companies continue to upgrade their digital operations, they leave themselves more vulnerable to attacks. Healthcare data continues to be more valuable than financial or personal data. As organizations continue to participate in digital transformations, scaling up their organization, and integrating the Internet of Things (IoT) or Internet of Medical Things (IoMT), the threat window for security issues widens and becomes more ominous; many cybersecurity teams now struggle to stay abreast of threats. In this age of digital growth, cybersecurity professionals must now consider data as the primary asset and analyze threats across systems, devices, and the cloud. Enterprises must maintain a strong and robust asset management program, become more resilient to cyberattacks, and generate business value by creating an advanced and strong cybersecurity program that protects their data from cyberattacks (Mishra & Gochhait, 2023).

Data as an Asset

Data is the primary asset in any medical center. Having a robust cybersecurity program is essential for protecting not only the patient data but also staff and data significant for the operation of the medical center such as financial or staff employee records. However, data must be classified or organized into tiers or classes so that security controls can be determined that manage and preserve the data against theft, unauthorized access (i.e., the most common data threat in the medical center), and improper retention or unsafe destruction of data such as throwing items which have not been deidentified into a garbage can (Warsinske et al., 2019). Once a data categorization policy and procedures have been developed and implemented, the medical center can then develop specific cybersecurity protocols based on the level of importance or sensitivity. For example, data in the medical center is classified as sensitive, confidential, private, public, or proprietary (i.e., patient data that has limited use outside of the facility such as billing data or patient data for research). Once data classification is finished, the medical center can categorize data, achieving two important functions: a) to establish risk tolerance and b) it assigns the value the organization places on the data (Warsinske et al., 2019). Customarily, asset management for information technology (IT) describes a set of practices in financial, inventory, and the lifecycle of an asset. IT assets are any devices used for business purposes (Burke, 2020). Medical centers are adopting the use of cloud technology, artificial intelligence (AI), IoMT, and other digital resources to protect against cyber threats and keep data safe. Web services, cell phones, biometrics such as fingerprint scanners, barcoding, etc., and other encrypted personal devices are just a few of the assets that a medical center must protect.

Cybersecurity for Asset Management

Asset management becomes vitally important the larger the organization. How the organization operates is another contributing factor to how strong a cybersecurity program must be. Most often, cybersecurity professionals working in these organizations suggest that cybersecurity programs be robust and that management continues to upgrade based on current threats (Norris et al., 2021). Cybersecurity has certain social, economic, and political effects that have only increased as medical centers have to worry about patient data, regulatory laws, privacy standards, and others. This should not be surprising as the digital world grows and data becomes not only richer, but more extended. However, some gaps still exist such as gaps in the knowledge base and an overall lack of clarity (i.e., noisy data, unstructured data, etc.). But at the same time, practitioners, cybersecurity professionals, and researchers must begin to think of data as an asset (Serrano, 2023). Asset management has been around for many years. Organizations must learn to preserve identify and categorize data to protect patients, staff, practitioners, and researchers. Organizations need to preserve data for legal or forensic reasons or privacy and to protect intellectual property. The steps necessary to build data retention and protect the data that is crucial to an enterprise begin with asset management and the individual or team designated to protect the data (Warsinske et al., 2019).

Network Components and Included Assets

Assets in Charleston Regional Medical Center include all the hardware and software in the three layers, APIs, and the Control Data Plane Interface demonstrated in Figure 1. Various software in the application layer is used for access controls, e-health, telehealth, patient monitoring, AI-driven applications, Big Data analytics, intrusion/attack detection, etc. The controllers in the control layer monitor, control, and manage the hardware in the infrastructure layer. The intelligent or smart assets provide enhanced functionality to the entire medical center. Improved functionality, including enhanced patient care, and in some cases, personalized medicine is enabled by Big Data analytics, AI, mobile apps, IoMT, etc. Superior patient care, personalized medicine in some cases, and reduced energy consumption are a result of a careful asset management program by the medical center. The main uniqueness is that technology and intangible assets can be standardized and subject to ubiquitous regulatory and ethical standards, while land, buildings, machines, etc. are subject to different standards and regulatory bodies (Serrano, 2023). In the infrastructure layer, assets include network devices, servers, storage devices, computing hardware, Internet of Things (IoT), Internet of Medical Things (IoMT), and machines such as barcoding scanners, fingerprint scanners, radio frequency identification (RFID) scanners, etc. IoMT can include medical devices, nurses' stations, etc. IoT, IoMT, barcoding scanners, and RFID scanners are used for data capture; fingerprint scanners are used for verification based on captured persons' fingerprints (patterns).

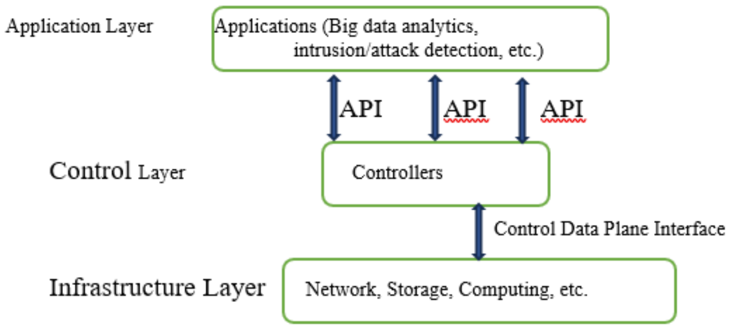
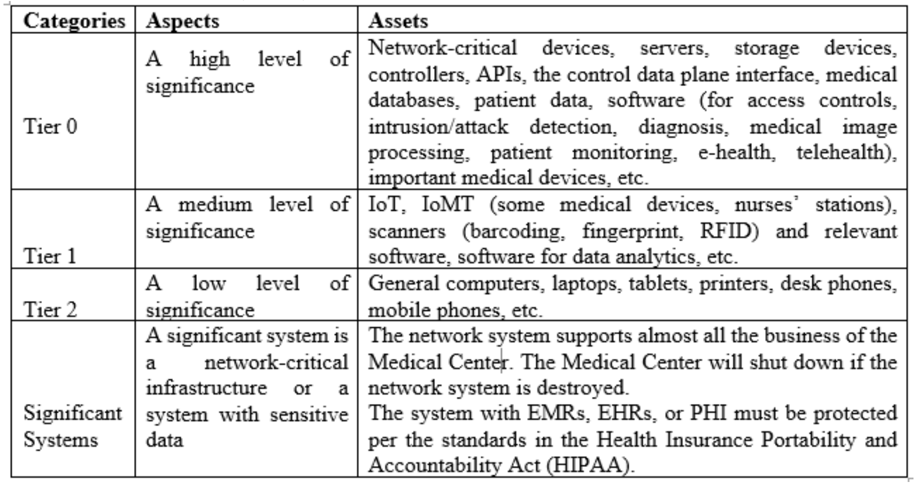

Application Layer
Applications (Big data analytics, intrusion/attack detection, etc.)
API
API
API
Control Layer
Controllers
Control Data Plane Interface
Infrastructure Layer
Network, Storage, Computing, etc.

Figure 1. Network Components in the Medical Center

Asset Classification in the Medical Center

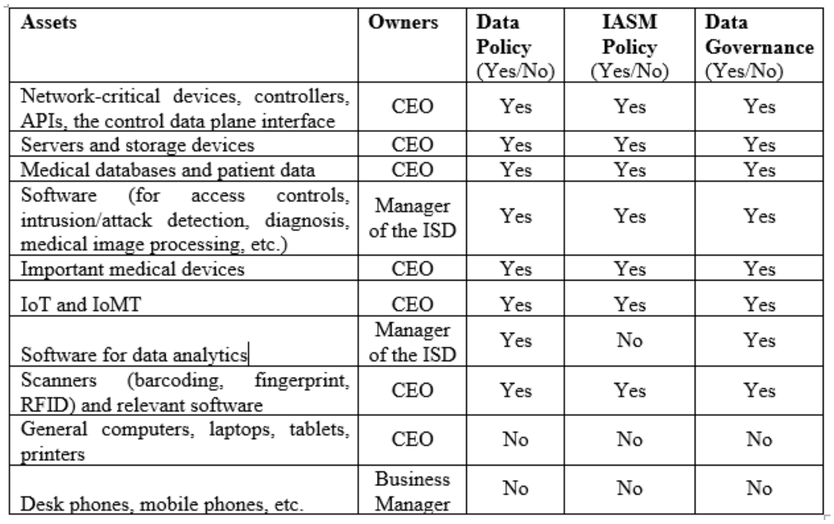
Table 1 shows information asset classifications in the Medical Center. Significant systems with a network or sensitive data, such as electronic medical records (EMRs), electronic health records (EHRs), or Protected health information (PHI) are described in the table. The significance level (high, medium, or low) for each asset is determined based on confidentiality, integrity, and availability.



Categories	Aspects	Assets
Tier 0	A high level of significance	Network-critical devices, servers, storage devices, controllers, APIs, the control data plane interface, medical databases, patient data, software (for access controls, intrusion/attack detection, diagnosis, medical image processing, patient monitoring, e-health, telehealth), important medical devices, etc.
Tier 1	A medium level of significance	IoT, IoMT (some medical devices, nurses' stations), scanners (barcoding, fingerprint, RFID) and relevant software, software for data analytics, etc.
Tier 2	A low level of significance	General computers, laptops, tablets, printers, desk phones, mobile phones, etc.
Significant Systems	A significant system is a network-critical infrastructure or a system with sensitive data	The network system supports almost all the business of the Medical Center. The Medical Center will shut down if the network system is destroyed. The system with EMRs, EHRs, or PHI must be protected per the standards in the Health Insurance Portability and Accountability Act (HIPAA).

Table 1. Classifications of Information Assets in the Medical Center

A chief executive officer (CEO), Board of Directors, Medical Board, or other authorized delegates have formal ownership responsibility. For example, a data owner is the person or group of individuals responsible and accountable for the data. A data owner sets rules for data utilization and data protection. A data policy outlines the guidelines for using, collecting, sharing, storing data, and destroying any data once it is no longer needed. An information asset security management (IASM) policy provides high-level, relevant guidance for the acceptable use of data, legal and regulatory considerations, and the roles and responsibilities of data users. The goal of data governance is to stop data-related problems before they arise (Warsinske et al., 2019). A data governance committee is created to ensure that data is protected under the statute, contract, or compliance/regulatory bodies. Table 2 shows the owners of assets, data policy, IASM policy, and data governance in the Medical Center. In Table 2, the owner of an asset can be the CEO of the Medical Center, the Business Manager, the Manager of the Information Security Department (ISD) in the Medical Center, or other authorized staff.

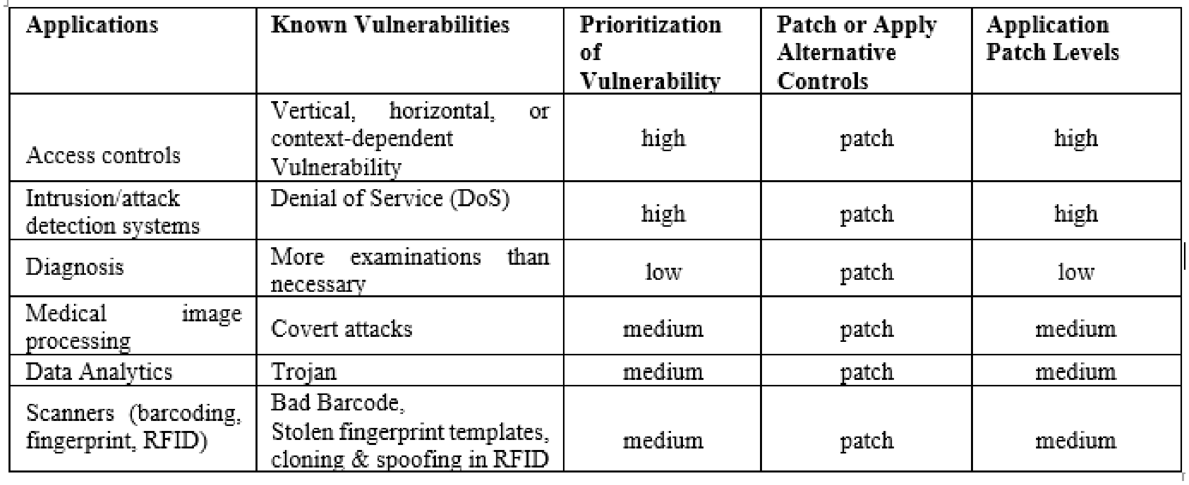


Assets	Owners	Data Policy (Yes/No)	IASM Policy (Yes/No)	Data Governance (Yes/No)
Network-critical devices, controllers, APIs, the control data plane interface	CEO	Yes	Yes	Yes
Servers and storage devices	CEO	Yes	Yes	Yes
Medical databases and patient data	CEO	Yes	Yes	Yes
Software (for access controls, intrusion/attack detection, diagnosis, medical image processing, etc.)	Manager of the ISD	Yes	Yes	Yes
Important medical devices	CEO	Yes	Yes	Yes
IoT and IoMT	CEO	Yes	Yes	Yes
Software for data analytics	Manager of the ISD	Yes	No	Yes
Scanners (barcoding, fingerprint, RFID) and relevant software	CEO	Yes	Yes	Yes
General computers, laptops, tablets, printers	CEO	No	No	No
Desk phones, mobile phones, etc.	Business Manager	No	No	No

Table 2. Owners of Assets, Data Policy, IASM Policy, and Data Governance

Software applications in the Medical Center mainly include access controls, intrusion/attack detection systems, diagnosis, medical image processing, data analytics, and scanners (barcoding, fingerprint, RFID). Software asset management includes vulnerability scanning and application patching for operating systems, third-party applications, and firmware. Patch management is a significant part of keeping software up-to-date and secure (Warsinske et al., 2019). Table 3 shows the inventory of software applications, the current list of known vulnerabilities, prioritization of each vulnerability by risk level (high, medium, and low), actions to patch or apply alternative controls, and application patch levels (high, medium, and low from software vendor if applicable). There are three main manifestations of access control vulnerabilities: vertical (sensitive functionalities), horizontal (also called lateral: resources), and context-dependent (resources and functionalities based on the application's context and user activity) (Zhong, 2023). There are different vulnerabilities in other software applications (see Table 3).

Actions to Patch or Apply Alternative Controls, and Application Patch Levels



Applications	Known Vulnerabilities	Prioritization of Vulnerability	Patch or Apply Alternative Controls	Application Patch Levels
Access controls	Vertical, horizontal, or context-dependent Vulnerability	high	patch	high
Intrusion/attack detection systems	Denial of Service (DoS)	high	patch	high
Diagnosis	More examinations than necessary	low	patch	low
Medical image processing	Covert attacks	medium	patch	medium
Data Analytics	Trojan	medium	patch	medium
Scanners (barcoding, fingerprint, RFID)	Bad Barcode, Stolen fingerprint templates, cloning & spoofing in RFID	medium	patch	medium

Table 3. Inventory of Software Applications, Vulnerabilities, and Their Prioritization, Actions to Patch or Apply Alternative Controls, and Application Patch Levels

Conclusion

Asset security is a fundamental process for an enterprise. By managing the assets, through identification and categorization, the enterprise can maintain asset security very well and identify any threats to the assets. For Charleston Medical Center, a mid-level facility, asset security involves data and identification of assets related to data security. For example, data mining equipment, servers, MIoT, IoT, the intranet, etc. The first task for asset management is to identify and organize the assets. RFID equipment, barcodes, templates, machine learning equipment, hardware, and software are all assets that are key to security. Some examples of cybersecurity breaches include staff who use electronic health records to keep up with family, neighbors, etc. Keeping the data secure and protected from cybercriminals is a crucial job for the IT department. It is also important to have cybersecurity on patch levels compliance—too high or too level can become an entrance for many crimes there.

Acknowledgements

The authors thank Technology & Healthcare Solutions, Mississippi, USA for its support.

Conflicts of Interest

There is no conflict of interest.

References

1. Burke, N. (2020). Why does asset management matter for cybersecurity? ISSA Journal, 13.
2. Mishra, S., & Gochhait, S. (2023, May). Emerging cybersecurity attacks in the era of digital transformation. In *2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 1442-1447). IEEE.
3. Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2021). Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity. *Journal of Urban Affairs*, *43*(8), 1173-1195.
4. Serrano, W. (2023). Smart or intelligent assets or infrastructure: Technology with a purpose. *Buildings*, *13*(1), 131.
5. 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.
6. Zhong, L. (2023). A survey of prevent and detect access control vulnerabilities. *arXiv preprint arXiv:2304.10600*.

DOI:10.31579/2639-4162/176