Acta Scientific COMPUTER SCIENCES

Volume 6 Issue 2 February 2024

Mini Review

# The Design of a Security Assessment and Testing Strategic Plan 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*

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

**Received:** January 12, 2024

**Published:** January 30, 2024

## Abstract

Healthcare facilities are highly susceptible to cyberattacks. With the increasingly digitalized healthcare enterprises, identity theft, medical records theft, and malware including Ransomware are just a few of the cybercrimes that have plagued medical centers over the last few decades. A security assessment and security testing include a security audit, assessment level, and vulnerability assessment to secure the health data that belongs to the medical center and patients of the medical center. Thieves are highly confident that using cybercrimes to steal medical data is lucrative because medical data is more valuable than a patient's social security number. Third parties can use confidential patient data to determine a patient's eligibility for insurance, hackers can use Ransomware to secure patient data for theft and the medical center would have to give the cybercriminals a hefty sum to release patient data. Assessment reporting is critical for the administrators, financial staff, IT staff, etc. to understand the depth of security assessments. This paper examines all these concepts and how to ensure that data is protected.

**Keywords:** Cybersecurity; Security Assessment; Security Testing; Security Audit; Assessment Level; Vulnerability Assessment; Assessment Reporting

## Introduction

Healthcare facilities can be vulnerable to cybersecurity attacks. Attacks can start in one area of the medical center and spread outward to others. For example, the lab may be attacked and then spread to all patient care areas lasting from hours to months. A multi-institutional, system-wide attack can lead to a shutdown of all patient care areas, ancillary service areas, and provider services such as secured mobile phone apps that contain patient data. Disruptions to patient care areas can lead to serious maltreatment and medical errors such as pharmacy, lab, x-ray, etc. Medication errors are the number one cause of lawsuits in the US. Due to the mechanization of medication dispensaries in hospitals, errors can occur and lead to disability and even death [1]. Because hospitals are becoming more and more dependent upon digital technology and electronic connectivity, cyberattacks are becoming more common. Hospitals are becoming the number one target of cybercrimes. Health information systems are common targets of those with Ransomware. Ransomware targets the mainframe and any connected devices including those in other facilities. It is quite possible that the number of attacks is higher than the number recorded. Hospitals are becoming more connected, larger, and more complex, leaving them more vulnerable to malware, including Ransomware [1].

Healthcare information security is not only the responsibility of the hospital but also lies with the individual owning the healthcare data. The importance of cybersecurity in healthcare facilities is becoming so much more important as the number of interconnected facilities increases. However, the likelihood of an attack is minimized by implementing security measures that mitigate risks. Risks such as data theft, Ransomware and malware attacks, and identity theft can be mitigated by staff training, powerful authentication measures, and critical follow-up activities that can predict attacks. It is critical that not only IT staff be trained for risk management, but also providers, other staff members, nurses, and other clinical staff [2].

### Medical center cyberattacks

Patient privacy is at the highest risk than ever. Cyberattacks have caused breaches in patient data and threats and additional risks to patients are also threats to patients' safety. Laying a firm foundation is imperative for preventing these damaging threats to patient data and preventing future attacks [3]. Considering the efficiency of healthcare data processing and indiscriminate testing of patients, annotation, and collection of samples, cyberattacks can cause a build-up or jeopardize patient safety by affecting patient care areas such as medication dispensaries (i.e., Pyxis, DynaMed, etc.) By keeping up a routine and robust cyberattack testing program and assessment, IT professionals can predict and prevent future attacks [4].

With the advent of big data in healthcare, precise and predictive healthcare has emerged from the healthcare system. Patients can be increasingly mobile with their healthcare, changing from facility to facility and essentially carrying important medical data with them. For example, Patient A may move to a new healthcare facility and carry that information with them. In the past, patient records may be late getting to new facilities, but currently, with the digitalization of records, transfer is almost instantaneous. With the advent of new 5G technology, the Cloud, Internet of Things (IoT) and Internet of Medical Things (IoMT), the elderly who are risk for falls, the patient most likely to develop diabetes, and the patient taking blood thinners can feel more comfortable as big data can help determine precise treatment. However, the patients' data can be at risk if an attack occurs [5]. New algorithms in patient care, testing, and artificial intelligence such as machine learning Neural Network (NN) algorithms can help mitigate further attacks. Precision attack training can help relieve such stressors on the system during pandemics (e.g., COVID-19 and other infectious disease breakouts), cancers, neurological diseases, and cardiovascular diseases [6]. Another aspect of the importance of training and testing security systems is the empowerment of employees to guard patient data from both internal and external attacks [7].

### Objectives and the scope of the assessment and testing strategy

The objective includes performing a quality security assessment and testing to ensure that robust cyber security and risk management is met in Charleston Regional Medical Center in the US. The detailed scope is as follows [8]: 1) testing the network system and hosts in the Medical Center; 2) regular vulnerability scans; 3) confidentiality, integrity, and availability; 4) assessment of cloud vendors, third-party service providers, or other organizations with business or services in the Medical Center; 5) assets tracking, including equipment, medical devices, data extraction devices, health data, etc.; 6) reviews of user files and logs; 7) privacy concerns about the collected data; 8) the susceptibility of employees to social engineering and relevant testing; 9) reviewing processes, standards, and documentation in the center; and 10) auditing and checking the adherence to policies, procedures, and standards.

### Assessment standards and assessment levels

The standard named 'The Statement on Standards for Attestation Engagements (SSAE)' is employed for the assessment in the Medical Center. SSAE 18 is the current version of the standard that presents Service Organization Control (SOC) reports (SOC 1, SOC 2, and SOC 3) [8]. The reports used in the Medical Center are shown in Table 1.

Both SOC 1 and SOC 2 can include either a Type I or a Type II audit. Type I is a point-in-time audit focusing on the design of controls. Type II is a period-of-time (over a longer time, three to 12 months) audit focusing on the design and operation of controls. A 12-month Type II audit period is standard. SOC 3 always implements a Type II audit. One crucial difference between SOC 2 Compliance and HIPAA (Health Insurance Portability and Accountability Act) is that HIPAA's requirements are not voluntary.

| SOC Levels | SOC 1 | SOC 2 | SOC 3 |
|---|---|---|---|
| Covered Items | Internal controls over financial statements and reporting | Confidentiality, integrity, and availability (CIA), as well as processing and privacy of customer data | SOC 2 results, tailored for the general audience |
| Reasons for Assessment | Audits of financial statements | Security, controls, risk mitigation, and compliance | Marketing to the public |
| Target Audience (Audit Users) | Financial executives, compliance officers, and financial statement auditors | IT executives, compliance officers, and regulators | General audience |
| Action Item Timeline | SOC 1 Type I financial audit takes place at a point in time.<br>SOC 1 Type II financial audit takes place over a period (12 months in the center). | SOC 2 Type I audit takes place at a point in time.<br>SOC 2 Type II audit takes place over a period (12 months in the center). | SOC 3 always implements a Type II audit, taking place over a period (12 months in the center). |

**Table 1:** Assessment levels, reasons, covered items, target audience (audit users), and action item timeline in the Medical Center.

### Assessment tools and procedures in the security assessment and testing

There are some automated tools that enable vulnerability scanning (scanning a range of IP addresses or a single host) and identifies vulnerabilities, missing patches, etc. Information Security Continuous Monitoring (ISCM) tools obtain data from many sources. This data may be integrated with Security Information and Event Management (SIEM) tools. GRC (governance, risk, and compliance) tools are very popular for security risk management. Integrating internal and external audit information could be performed through audit management tools [8]. The procedures in the assessment and testing include audit review, analysis, and reporting. Specifically, the procedures cover the backup of the information system; contingency plans; backup storage location(s); determination of the adequacy of security and privacy measures; and identifying security and privacy deficiencies [9].

### Impacts of the security assessment and testing

Specifically, the impacts on the Medical Center lie in: 1) ensuring the systems are running normally and there is a robust cyber security plan; 2) improved services and policies adherence—employees and IT professionals follow the policies and procedures such as deidentification of data for research and testing, prevention of data escape during testing; and 3) making certain that medical practitioners practice safe and personal care to patients.

### Vulnerability assessment, scanning tools, and goals for implementation

A vulnerability assessment process is identifying and then categorizing and assessing vulnerabilities. Vulnerability scans (checking assets for known vulnerabilities) are conducted. Assets can be servers, routers, operating systems, their installed applications, and healthcare data, etc. [8]. Many scanning tools can disable unsafe checks. The scanning tool must be configured with the credentials needed to log in. Implementation goals are to reduce traffic on the network and improve vulnerability identification [8].

### Reporting security assessment and testing findings

The reporting offers visibility for Medical Center officials into weaknesses and deficiencies in security or privacy controls [9] in the center. An executive-level report without technical details needs to be finished. A second report with technical details is needed too for remediation efforts. The peer review of the reports is critical. Executives generally do not have the time or interest to review technical details. However, a server administrator or other IT professional needs to remediate vulnerabilities and is interested in the details [8]. Therefore, an executive-level report is forwarded to executives while the second report is sent to the server administrator or IT professional.

## Conclusion

Over the last few decades, the electronic digitalization of healthcare records, the electronic medical record (EMR), and other electronic healthcare records has opened medical centers up for all types of phishing, malware, Ransomware, etc. With the advent of big data, blockchain, and IoT and IoMT, there has been an explosion of identity theft, medical record theft, and other types of cybersecurity breaches. With each breach, there is a chance for serious medical errors to occur. With the pharmacy digitalized and patient care dependent upon the Internet, errors in medicating the patient can occur as well as misdiagnosis and abnormal treatments which can lead to lawsuits or even the death of a patient. With an aggressive plan for security assessment and a plan to securely test the cybersecurity plan, staff, provider, and clinical staff training, can prevent serious or deadly errors. It is critical that a plan be in place for preventing cyberattacks and for IT professionals to guide clinical staff in preventing internal and external attacks.

## Acknowledgements

Authors thank Technology and Healthcare Solutions, Mississippi, USA for support.

## Conflicts of Interest

## Bibliography

1. Stowman AM., *et al*. “Anatomy of a cyberattack: Part 1: Managing an anatomic pathology laboratory during 25 days of downtime”. *American Journal of Clinical Pathology* 157.4 (2022): 510-517.
2. Javaid M., *et al*. “Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends”. *Cyber Security and Applications* (2023): 100016.
3. Bhuyan S S., *et al*. “Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations”. *Journal of Medical Systems* 44 (2020): 1-9.
4. Li Y., *et al*. “Healthcare Data Quality Assessment for Cybersecurity Intelligence”. *IEEE Transactions on Industrial Informatics* (2022).
5. Lai J., *et al*. “Edge intelligent collaborative privacy protection solution for smart medical”. *Cyber Security and Applications* 1 (2023): 100010.
6. Abernethy A., *et al*. “The promise of digital health: then, now, and the Future”. National Academy of Medicine (NAM) perspectives, June 27 (2022): 1-24.
7. Radanliev P and De Roure D. “Advancing the cybersecurity of the healthcare system with self-optimising and self-adaptative artificial intelligence (part 2)”. *Health and Technology* 12.5 (2022): 923-929.
8. Warsinske J., *et al*. “The Official (ISC) 2 Guide to the CISSP CBK Reference”. John Wiley and Sons (2019).
9. Joint Task Force Transformation Initiative. Assessing security and privacy controls in federal information systems and organizations: building effective assessment plans (No. NIST Special Publication (SP) 800-53A Rev. 4 (Withdrawn)). National Institute of Standards and Technology (2014).