Cybersecurity Trends in Health Information Systems

Ahmad Mustafa Mohamad Al-Aboosi
Siti Norul Huda Sheikh Abdullah
Mohd Zamri Murah
Faculty of Information Science and Technology
Universiti Kebangsaan Malaysia (UKM)
Email: ahmad_aboosi@yahoo.com,
snhsabdullah@ukm.edu.my, zamri@ukm.edu.my

Ghassan Saleh ALDharhani
Institute of Computer Science
& Digital Innovation (ICSDI)
UCSI University, Malaysia
ghassan@ucsiuniversity.edu.my

***Abstract*—Health information systems are vulnerable to cyber attacks, which is expected to increase exponentially. Cyber attacks with different attack techniques present great difficulties for professionals who have been exploring techniques to overcome security weaknesses. The aim of this paper is to examine cybersecurity trends in health information systems, including current threats and their relevance to health information systems. The article focuses on common threats from cyber attacks, such as ransomware, Denial of Service (DDoS) attacks, and Denial of Service (DoS). Secondly, we propose mitigation processes to reduce or eliminate the risk of cyber attacks. A security assessment can be performed to determine the risks of cyber attacks. The health organization must classify the risk according to criticality, determine the main cause of the risk, and recommend appropriate procedures and security controls. Health organizations should do more to support their cybersecurity programs.**

***Keywords*—healthcare information system, cyberattacks, cybersecurity**

I. Introduction

In recent years, the use of health information systems in the medical field has increased significantly [1]. Electronic medical records are organized and managed by health information systems. Electronic medical records can be obtained from multiple sources within a single health care facility. These records contain information on patient treatments, diagnostic procedures, laboratory tests, medical history, prescriptions, and allergy issues [2]. As the health industry digitizes to maintain its health, it cannot adopt technological security features at the same rate, leaving healthcare information systems vulnerable. 41% healthcare organizations, including credit / debit card information and medical records, have more than 1,000 confidential and unprotected files. Seventy percent of the health sector claim to have been severely injured by cyberattacks. Health information systems are the most susceptible to ransomware attacks, which are expected to increase exponentially [3].

Cyber attacks are the most common cause of medical data breaches, where the various attack techniques pose significant challenges to security professionals who have been exploring ways to overcome security weaknesses [3]. Medical records are valuable to cyber criminals because they contain social security and credit / debit card numbers, demographic data from patients, addresses, insurance identification numbers, and other health information. This information can be used to create false identification for drug purchases or insurance fraud. Consequently, the protection of medical records is crucial [4], [5].

Understanding the factors and causes behind the security background and persistent data breaches is essential for a safer and more secure healthcare industry. This is the result of the security approaches of the healthcare industry, which, while robust, are frequently less advanced than those of other industries, such as the financial sector [6].

The purpose of this paper is to investigate cybersecurity trends in health information systems, including the most significant current threats and their applicability to health information systems. It is organized as Section I for the introduction, Section II for attacks in the healthcare domain, Section III for security failure factors in healthcare, Section IV for the health information security test, Section V for recommendations, and Section VI for the conclusion.

II. Cyber attacks In Health Care domain

A systematic study of cyber security in healthcare agrees with the growing threat of cyber attacks in healthcare care and the systemic lack of preparedness to deal with cyber threats [7]. Many IT experts are concerned that recent trends will convince cyber criminals to target medical devices such as pacemakers or respiratory machines from the intensive care unit (ICU) [8]. According to the 2021 HIMSS Healthcare Cybersecurity Survey, the most serious security breaches were phishing or ransomware attacks, and these attacks often make headlines when healthcare organizations are targeted by cybercriminals [9].

Despite this, the healthcare industry may be more concerned with phishing and ransomware attacks than other potentially dangerous types of attack. The following are the most prevalent attacks on healthcare systems.

Research grant: GUP-2020-087

2022 International Conference on Cyber Resilience (ICCR) | 978-1-6654-6122-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICCR56254.2022.9995952

A. Phishing attack

Phishing is a technique in which an attacker attempts to steal personal information from a user to use it fraudulently. There are currently three strategies to counter such threats: Increased focus on awareness, blacklists, and machine learning [8]. According to HIMSS, the most serious security issue is frequently phishing, General email phishing (71% of the respondents), spear phishing (67%), phishing/voice phishing (27%), whaling (27%), hacking company email (23%), SMS phishing (21%), phishing websites (20%) and social media phishing were the forms of phishing mentioned (16 %) [10].

All employees can receive security awareness training to reduce the risk of phishing attacks in healthcare organizations. And not once or once a year, but on a regular basis through training, webinars, correspondence, and reminders. Multifactor authentication is an additional requirement for access to software and IT services. Even if the employee provides his credentials, attackers will still have to devise a more secure authentication method. Endpoints must be protected by anti-malware software, and some phishing attacks will be successful through endpoint detection and response [9].

B. Ransomware

Ransomware is a type of virus that attackers use to encrypt files and demand a ransom in exchange for the decryption key. These ransoms are often demanded in bitcoin or another cryptocurrency. Ransomware remains one of the most prevalent threats facing healthcare security companies. With this new coercion scheme, ransomware such as Sodinokibi, Ryuk, DopplePaymer, and Egregor have begun to threaten their victims. Several organizations have issued coordinated cybersecurity advice to inform hospitals and healthcare professionals in the United States about ongoing ransomware attacks during the COVID19 outbreak [11].

C. DDoS Attacks

The most effective attack on the availability of patient health data and healthcare services is a distributed denial of service (DDoS) attack. A DDoS attack has a significant impact on the capacity and performance of the healthcare network [12].

Hackers make services inaccessible through a malicious attack. Denial-of-Service (DoS) attacks primarily interfere with certain healthcare assets. Although there are numerous types of denial-of-service attacks, such as flood attacks, amplification attacks, protocol exploit attacks, and malformed packet attacks, they are all, in essence, different forms of asset flooding with traffic to the point where a device is denied service. Although it is impossible to prevent a hacker from attempting to launch a DDoS attack, proper preparation, such as a response plan and preventive measures such as limiting network broadcasting, cloud-based protection, continuous monitoring, and server redundancy, can mitigate the attack's potential risks and effects.

III. Healthcare Security failure Factors

A. Low access control management

Restricting access to information is the most important factor in the security success of any healthcare organization. Access to personal health records should be controlled at all stages of a health facility, according to a study published by the US Department of Health and Human Services [13]. Instead of sharing a small temporary database, many healthcare organizations share their master database with other agencies and colleagues. The main reason for this problem is the lack of resources and time [14]. Typically, breaches involve internal employees. To maintain a low rate of data breach risk and a high rate of security, access control in the healthcare industry must be restricted and rebuilt.

B. Outdated Infrastructure(software/Hardware)

In the healthcare industry, technical information technology equipment is lag behind obsolete IT infrastructure. Every system and piece of equipment must be upgraded for optimal performance and security. However, in the context of the healthcare industry, it is often observed that the technical infrastructure is burdened by an outdated IT landscape. This type of vulnerability provides an open door for attackers to exploit smart healthcare services.

Every system and device must be updated for proper and secure operation. In the context of a healthcare organization, it is customary to examine the technology infrastructure that supports legacy IT situations. This threat gives attackers the opportunity to exploit the services of the health information system.

C. Human error

Some of the reported medical data breaches can be attributed to poor communication and coordination, incorrect instructions, or previous signs of mental overload due to exhaustion, concentration, or stress. Human error is the most difficult to consider. It can have a significant impact on the system if it occurs at the organization's access level. With adequate training and enhanced human knowledge, organizations can avoid this problem.

D. inadequate security defenses

Many documented data breaches indicate that the impact of a data breach can be mitigated if defensive security concerns are addressed in advance [15], [16].

E. Social Engineering

Social engineering is the most effective weapon in health information systems against targets. If a medical facility employee exhibits a particular online behavior, attackers can gather information about employees through their behavior, environment, social media portals, and casual interactions with employees. This information could be used by an attacker to target the user.

F. low compliance with policies and standards

Therefore, effective health information system security requires that employees are aware and also comply with health information system security policies and guidelines.

IV. Health Information System Security Assessment

Before attackers breach the healthcare system, security professionals can access the network or other IT infrastructure to determine the possibility of a threat by identifying and documenting potential vulnerabilities and threats. Because security testing is effective, the Health Insurance Portability and Accountability Act (HIPAA) and other security regulations encourage or mandate that healthcare providers perform it.

A. Footprinting

Footprinting is the process of collecting data on target systems, such as servers, PCs, routers, switches, medical and IoT devices, operating systems, applications, and firewalls, and about personnel information, such as names, family names, social security numbers, birthdays, addresses, phone numbers, and emails, using various techniques, such as online directories, search engines, social engineering, behavior monitoring by monitoring personnel behavior such as shoulder surfing, and monitoring personnel behavior by monitoring personnel behavior, such as shoulder surfing. The weaknesses of the health information system will be determined by analyzing these data. Raising employee awareness, limiting sensitive information, using privacy services in the Whois lookup database, disabled directory listings on web servers, and enforcing security policies are methods to prevent footprinting of health information systems and personnel data.

B. Enumeration

Enumeration is the next step in testing health information systems and involves scanning and exploring healthcare networks or websites in real time using network scanner tools such as Nmap, Angry IP Scanner, Zenmap, Advanced IP Scanner, and MASSCAN for current vulnerabilities, especially if the system is not updated to the latest version. The enumeration can be used to obtain misconstrued resources and software versions with known vulnerabilities, such as outdated operating systems or applications.

C. Vulnerability scanning

Vulnerability scanners, such as Grendel-Scan, Wapiti, W3AF, OpenVAS, Acunetix, N-Stalker, Netsparker, and Burp Scanner, are defined as software that assesses whether security weaknesses and vulnerabilities may be relevant to the operation of a target website or network, also known as vulnerability analysis, some of the features offered by vulnerability scanners such as defining and categorizing target systems, assigning rankings in proportion to device assets, determine potential asset risks, create a strategy to deal with the most serious issues, and defining and implementing processes to mitigate the impact of attacks on target systems.

To construct a safe and reliable health information system, they must employ vulnerability indicators to track, assess, and measure the activity of the system in numerous vulnerabilities and attacks. Vulnerability scanning systems are specific because they require an active understanding of the target, such as health information systems, to be tested to succeed. This includes the use of a network scanner, a host scanner, a server scanner, or a web application scanner.

D. SSL Analysis

As healthcare systems continue to transform their organizations into the digital world, especially those providing access over the Web, the need for SSL encryption is crucial to stay safe. Information sharing without SSL poses significant risks and may lead to leakage of sensitive information data, SSL is a client-server protocol that includes authentication, encryption, and decryption mechanisms. There are two important functions: at the beginning of the session, the authentication of the server and the client, and the encryption and decryption of the data exchanged by both parties [17].

It is important to periodically verify the validity and credibility of the SSL certificate. In addition, to check the support for protocols, key exchange, cipher, and provide an overall level of SSL, you need to use one of the SSL checking tools like Qualys SSL Lab and SSL Checker.

E. Privacy and Security Policy Content Analysis

Health information systems are a vital part of healthcare organizations. They provide a means for patients to access their health information and communicate with their healthcare providers. To ensure that patients have confidence in these systems, security and privacy policies must be established and enforced.

The Security Policy ensures the security of the system, while the Privacy Policy describes how personal information is kept and used. Both must communicate and interact with these strategies to support the health information system. When healthcare organizations do not enforce or publish their rules, patients worry about the trust and transmission of their information. Once the policy is established, it must be followed and maintained.

An organization's reputation can be improved by establishing adequate security policies. Lower costs can be incurred by implementing security measures, and faster incident response times can result from having a well-designed security plan. However, if an organization does not establish adequate security, its competitive position can be adversely affected.

Health information systems must implement and enforce sophisticated security policies to protect confidential data and activities from common vulnerabilities such as weak authentication, cross-site fraud, cross-site programming, and SQL injection. By doing so, organizations can improve their reputation, reduce costs, and respond more quickly to incidents.

F. Compliance with Security Standards

Security standards are guidelines used for asset protection management. A standard consists of a set of policies that

are defined, constructed, developed, and maintained based on software, hardware, and other asset resources. These policies control the use of assets' resources.

Organizations should conduct regular compliance checks with security standards to understand the latest regulations that must be applied in health information systems and to determine whether they comply with health and security standards such as HIPPA, ISO 27000 series (e.g., ISO/IEC 27001), ISO 27799:2008 (Health informatics - Security management in healthcare delivery organizations) or HITRUST CSF common security framework). Exceptions to rules and procedures should be kept to a minimum because they can significantly weaken the security posture of any healthcare facility.

G. Evaluation and reporting

The evaluation of the security assessment is important to ensure the safety of health information systems. By classifying risk according to criticality, determining the main cause of the risk, and recommending appropriate procedures and security controls, the report helps improve the security of the system. The scope and techniques used by the assessors during the surveillance assessments are also described in detail, along with findings and suggestions to address any vulnerabilities or flaws discovered. This report provides valuable information for anyone responsible for ensuring the safety of health information systems.

V. Recommendations

The security of health information is a top priority for healthcare organizations. A strong foundation of basic security controls is essential to protect patient data. Without these controls in place, providers will not be able to reach its full potential. Healthcare organizations are recommended to implement basic and advanced security controls to ensure a high level of protection against potential attacks and data breaches. Some of the most effective security measures include antivirus/antimalware solutions, firewalls, email security gateways, encryption, patch and vulnerability management, network monitoring tools, web security gateways, intrusion detection and prevention systems (IDPS), privileged access management, data loss prevention systems (DLP), single sign-on (SSO), mobile device management (MDM) and zero trust solutions.

Implementing an effective cybersecurity program can be a challenge for any organization, but it is especially challenging for healthcare organizations due to the sensitive nature of their work. However, by taking steps to improve their cybersecurity posture through the implementation of strong safety measures such as those outlined above, healthcare organizations can better protect themselves against the ever-evolving threats of today.

VI. Conclusion

Healthcare organizations still have significant challenges to overcome. These barriers to progress include tight security budgets, growing legacy footprints, and the growing volume of cyber attacks and compromises. Additionally, basic security controls have not been fully implemented in many organizations. But perhaps the greatest vulnerability is the human factor. Healthcare organizations should do more to support healthcare cybersecurity professionals and their cybersecurity programs.

References

[1] J. Adamu, R. Hamzah, and M. M. Rosli, "Security issues and framework of electronic medical record: A review," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 2, pp. 565–572, 2020.

[2] G. Amirthalingam and H. Thangavel, "Multi-biometric authentication using deep learning classifier for securing of healthcare data," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 4, pp. 1340–1347, 2019.

[3] A. Razaque, F. Amsaad, M. J. Khan, S. Hariri, S. Chen, C. Siting, and X. Ji, "Survey: Cybersecurity vulnerabilities, attacks and solutions in the medical domain," *IEEE Access*, vol. 7, pp. 168 774–168 797, 2019.

[4] R. E. Moffit and B. Steffen, "Health care data breaches: A changing landscape," *Maryland Health Care Commission*, pp. 1–19, 2017.

[5] N. Kagalwalla, T. Garg, P. Churi, and A. Pawar, "A survey on implementing privacy in healthcare: An indian perspective," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 3, pp. 963–982, 2019.

[6] P. Vimalachandran, H. Wang, Y. Zhang, B. Heyward, and Y. Zhao, "Preserving patient-centred controls in electronic health record systems: A reliance-based model implication," in *2017 International Conference on Orange Technologies (ICOT)*. IEEE, 2017, pp. 37–44.

[7] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," *Technology and Health Care*, vol. 25, no. 1, pp. 1–10, 2017.

[8] E. Benavides, W. Fuertes, S. Sanchez, and M. Sanchez, "Classification of phishing attack solutions by employing deep learning techniques: A systematic literature review," *Developments and advances in defense and security*, pp. 51–64, 2020.

[9] R. Abdillah, Z. Shukur, M. Mohd, and M. Z. Murah, "Phishing classification techniques: A systematic literature review," *IEEE Access*, 2022.

[10] G. Saira, S. Arvind, and D. Mike, "Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that," *Digital Health*, vol. 8, p. 20552076221104665, 2022.

[11] N. Spence, M. Niharika Bhardwaj, and D. P. Paul III, "Ransomware in healthcare facilities: a harbinger of the future?" *Perspectives in Health Information Management*, pp. 1–22, 2018.

[12] H. Abbas, R. Latif, S. Latif, and A. Masood, "Performance evaluation of enhanced very fast decision tree (evfdt) mechanism for distributed denial-of-service attack detection in health care systems," *Annals of Telecommunications*, vol. 71, no. 9, pp. 477–487, 2016.

[13] U. D. of Health, H. Services *et al.*, "Health industry cybersecurity practices: Managing threats and protecting patients," 2020.

[14] A. K. Pandey, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal, R. Kumar, and R. A. Khan, "Key issues in healthcare data integrity: Analysis and recommendations," *IEEE Access*, vol. 8, pp. 40 612–40 628, 2020.

[15] A. A. Ali and M. Z. Murah, "Security assessment of libyan government websites," in *2018 Cyber Resilience Conference (CRC)*. IEEE, 2018, pp. 1–4.

[16] M. Z. Murah and A. A. Ali, "Web assessment of libyan government e-government services," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 12, 2018.

[17] A. M. M. Al-Aboosi, S. Kamil, S. N. H. S. Abdullah, and K. A. Z. Ariffin, "Lightweight cryptography for resource constraint devices: Challenges and recommendation," in *2021 3rd International Cyber Resilience Conference (CRC)*. IEEE, 2021, pp. 1–6.