IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A comprehensive Study To Identify The Knowledge And Awareness Of Cyber Security Attacks In The Digital Health Care

[1]Mohammed Mukkaram Ali, [2]Fazeela Tunnisa, [3]Shiraz Ahmed Maniyar

[1]Lecturer, [2]Lecturer, [3]Lecturer

[1] Department of Computer, [2] Department of Computer Science, [1] Department of Health Informatics

[1]Jazan University [2]Jazan University [3]Jazan University, Kingdom of Saudi Arabia

Abstract: This study has been undertaken to study the Security for Digital Healthcare system. It is important for all health organizations and impersonals. Highly Digitalized Medical Devices and Healthcare apps are significant to patient care, but there is a probability of disruption of valuable data targeted by hackers, so there is need to implement cyber security awareness among medical practitioners and patients. Cyber security in the digital healthcare systems pertain to different types of threats against Innovative Medical devices. One of the aim of this study to identify threats and vulnerabilities and provide cyber security solutions to safeguard health information from hackers.

Keywords: Information technology Cyber-attacks, Cyber security, Health care, Key management

1. Introduction

Cyber security awareness is a critical business issue for every organization. However, it is quite simply essential in the healthcare sector, where data is particularly sensitive. The large volumes of confidential data, combined with often vulnerable security systems, and an extensive network of connected medical devices make the healthcare sector a prime target for cybercriminals. The healthcare industry is one of the most exposed industries, plagued by a myriad of cyber security-related issues, such as security incidents, organizational breaches, and data theft originating from internal and external sources.

2. Related Work

2.1 Cyber Security Concerns in the Healthcare Sector

It is clear that hackers will continue to launch cyberattacks targeting the healthcare industry while there are profits to be made, whether selling stolen patient data or holding healthcare systems hostage until the criminals' demands are met. The healthcare sector has experienced a significant shift in recent years with the adaptation of new technologies to facilitate data integration, patient engagement, and clinical support.

With this transition from traditional paper-based methods comes a wealth of opportunities for cybercriminals, such as malware that compromises the privacy of patient data, to distributed denial of service (DDoS) attacks that disrupt the ability to provide patient care. However, organizations are often too preoccupied with defending against external threats to address the very real and dangerous risks that may lie within their own ranks.

3. Main Threats

Cyber security in the healthcare industry should be particularly concerned about the following threats:

(a) Ransomware

In addition to encrypting data and demanding money to decrypt it, criminals block access to the entire clinical system, rendering surgical instruments and life support equipment inoperable.

(b) Phishing

Computer systems can become infected with malware through links or attachments in phishing emails, social media posts, or text messages, frequently spreading over the entire network.

(c) Network vulnerability attacks

ARP cache poisoning, HTTPS spoofing, and other cybercrimes target the wired and wireless networks that are the lifeblood of medical facilities and give access to patient data.

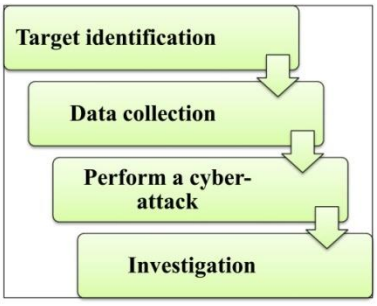
(d) Man-in-the-middle (MITM) attacks

Cybercriminals snoop on private (and very important) user information during data transfers or discussions, resulting in significant losses and fines for a confidentiality breach.

(e) Data Breaches

Comparatively speaking, the healthcare sector has a disproportionately high number of data breaches. Although efforts to limit these occurrences through frameworks like HIPAA, such as cybersecurity gaps, give cyber attackers access points via which they can continue to compromise the security of medical care data.

This figure shows the study of a Cyber Attack



4. Cyber attacks against Medical Devices

Healthcare IT experts find it particularly difficult to maintain security because of the enormous number of linked medical equipment, many of which have different specifications and come from different manufacturers. Even though medical devices don't necessarily include a lot of patient data, they can serve as easy access points for hackers to servers containing a lot of data. The healthcare cybersecurity market must prioritize keeping these entry points securely and up to date to reduce the costs and harm brought on by unauthorized access.

5. Cyber security Solutions for the Healthcare Industry

Here are several security precautions that can be taken as cybersecurity for hospitals and healthcare facilities to safeguard electronically protected health information (ePHI) by defending tools, digital systems, networks, and data from threats as a healthcare cybersecurity solution.

5.1 Control of data consumption

Malicious file activity should be contained and observed by clinics. They can achieve this by putting in place systems that restrict access to data, stop unauthorized emails from being shared, block copies to external sources, etc.

5.2. Record data

Keep track of information to spot unauthorized access to patient files immediately. Logs will assist a clinic in a cyberattack by allowing them to identify and close the quick breach.

5.3. Impose stringent access restrictions

They must use a password/PIN, cards and keys, face, fingerprint, or retina recognition to protect patient data from illegal operations.

5.4. Apply cutting-edge cryptography

To encrypt data during transmission and storage, use modern cryptography. Some examples are homomorphic encryption, secure multiparty computation, or distributed ledger systems.

6. Use of Cyber security in Healthcare Laws and Regulations

Government and industry agencies have developed compliance standards and guideline frameworks, such as: to aid healthcare firms in protecting vital assets and data from healthcare cyber threats.

6.1. Privacy and general safety

A common set of consensus-based, voluntary, and industry-led guidelines, best practices, methodologies, procedures, and processes" are provided in "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients" by HHS and Healthcare and Public Sector Coordinating Councils to aid healthcare cybersecurity regulations.

National standards established under the HIPAA Security Rule safeguards people's electronic personal health information (ePHI). The Security Rule requires compliance with administrative, physical, and technical protections, including, among others, access control, to ensure the integrity, confidentiality, and security of ePHI.

The HIPAA Security Rule standards and implementation requirements are mapped to the relevant NIST Cybersecurity Framework sub-categories in NIST's "HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework" document.

7. How to prevent cyber-attacks in healthcare

The adoption of cutting-edge technology by healthcare organizations has increased recently. Examples include AI, big data, VR and AR, blockchain, etc. They can offer superior patient care and diagnostic services because of the advancements that help medical facilities work more effectively and are some of the cybersecurity trends in healthcare.

7.1. Internet of Things (IoT) and smart devices to transform patient care

The Internet of Things already impacts the patient and doctor sides of healthcare. Patients can monitor their health through the connectivity of devices like electrocardiograms, thermometers, glucose monitors, ultrasounds, and more. Moreover, many hospitals are now using "smart beds," which include sensors that can sense the presence of a patient and modify themselves to provide the right support without requiring a nurse to step in the healthcare cybersecurity market size. The Internet of Things can also improve at-home patient care. Smart medication dispensers, for instance, can notify doctors when patients don't take their medication and immediately upload information to the cloud. More generally, IoT technology in healthcare enables clinicians to be aware of any potentially risky patient behavior.

7.2. Automated diagnosis using Artificial Intelligence (AI)

By utilizing medical knowledge that AI systems have thoroughly evaluated and memorized, AI in healthcare will help healthcare practitioners improve patient outcomes. These systems can deliver therapeutically pertinent information to doctors and researchers using data in electronic health records for urgent requirements. Cognitive systems that generate real-time 3D visuals are intended to enable the rapid diagnosis of serious illnesses like cancer and diabetes. They could spot recognizable physiological traits in the scans. AI systems provide patients with readily available, reasonably priced, and high-quality care. It helps in the prevention of healthcare cybersecurity attacks.

7.3. Blockchain to improve the security of health data

By improving the security, interoperability, and privacy of health data, blockchain technology has the potential to revolutionize the healthcare sector. By increasing the effectiveness and removing intermediaries from electronic medical records, the application of this technology in healthcare could offer a new framework for health information exchanges. Additionally, because every link in the chain must confirm a transaction before it can be accepted, block chain can address the identity management issue, which might promote innovation in the healthcare industry. For instance, the Ether unblock chain can be used by a system called MedRec to maintain medical records. It qualifies as a clinical and research block chain since it grants users access to census-level data from medical records.

8. Take steps to protect your organization

The cyber bad guys spend every waking moment thinking about how to compromise your cybersecurity procedures and controls. The best defense begins with elevating the issue of cyber risk as an enterprise and strategic risk-management issue. If possible, you should also dedicate at least one person full time to lead the information security program, and prioritize that role so that he or she has sufficient authority, status and independence to be effective. Furthermore, you and your team should receive regular updates on your organization’s strategic cyber risk profile and whether adequate measures are dynamically being taken to mitigate the constantly evolving cyber risk.

Finally, the most important defense is to instill a patient safety-focused culture of cybersecurity. This enables health care organizations to leverage their existing culture of patient care to impart a complementary culture of cybersecurity. A culture of cybersecurity, where the staff members view themselves as proactive defenders of patients and their data, will have a tremendous impact in mitigating cyber risk to the organization and to patients.

As senior advisor for cybersecurity and risk for the American Hospital Association, I am available to assist your organization in uncovering strategic cyber risk and vulnerabilities by conducting an in-depth cyber-risk profile, and by providing other cybersecurity advisory services such as risk mitigation strategies; incident response planning; vendor risk management review; and customized education, training and cyber incident exercises for executives and boards.

8.1 How to Prioritize Cyber Threat Prevention in Healthcare?

Cyberattacks are a persistent concern in today's top healthcare cybersecurity companies. It has demonstrated the value of prioritizing the remediation of Cybersecurity threats.

a. Get the Stakeholders Involved in the Process

Remediation of cybersecurity threats is frequently entrusted to the "IT guys". Stakeholders, including those in senior management roles and those with distinctive viewpoints, experiences, and talents that IT may not possess, are crucial in determining how to prioritize addressing cybersecurity threats.

b. Find threats to your online security

Determine the danger categories, scenarios, and occurrences when identifying cybersecurity threats. Threat categories are sophisticated classifications that identify dangers in important IT functions. Determine the danger scenarios or typical situations for each threat category after determining the threat categories. Threat events are particular weaknesses under a given threat scenario.

c. Decide what level of risk is tolerable and unacceptable

Set a limit for what constitutes an acceptable and unacceptable level of risk for the organization. This limit should have a specific monetary value determined by the organization's capacity for accepting financial losses and risk tolerance.

d. Create a scale to measure the financial impact

A similar financial impact results from cyberthreat. If senior management is unsure of the financial implications of cybersecurity concerns, it is difficult for them to make wise judgments. It is crucial to develop a scale to evaluate the economic effect of each dangerous event that has been detected.

e Establish a probability scale

Make a scale to measure the likelihood that each hazard event will occur over a specific period. Verify that the probability scale has an equal number of levels as the scale measuring economic effect.

f. Assessment of the level of threat

Determine the severity level for each danger event. Multiply the cost of the financial impact by the likelihood that it will occur to determine the threat level severity for each threat event.

f. Find out how close the threat event is

The financial impact and likelihood of a threat event changing over time are frequently variable. Threat proximity is the link between a threat's likelihood and its timing. Occasionally, these variations are unpredictable. However, some threat events can be anticipated. The danger of losing essential employees is always present. Before the release of a new product, there is a limited window of opportunity for data breaches. After a certain time, the chance of a project going over budget significantly after staff reductions either increases or decreases.

8. REFERENCES

https://www.sciencedirect.com/science/article/pii/S2352484721007289

https://cltc.berkeley.edu/scenario-back-matter/

https://www.bitdegree.org/tutorials/what-is-cyber-security/