Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI:10.21474/IJAR01/19459
DOI URL: http://dx.doi.org/10.21474/IJAR01/19459

RESEARCH ARTICLE

CYBERSECURITY IN CLINICAL PRACTICE

Prof (Dr.) Anu Gauba
Professor, Amity College of NursingAmity University, Gurgaon.

Manuscript Info

Manuscript History
Received: 15 July 2024
Final Accepted: 17 August 2024
Published: September 2024

Abstract

Cybersecurity is a concern for patient safety. Recent cyberattacks on healthcare facilities around the world have exposed the risks to patients: from treatment delays due to hospital and clinic closures, to the threat harm from personal data theft, to patient death. The recent Covid-19 pandemic has further increased cyberattacks against healthcare organizations. Frontline healthcare workers are often warned about the dangers of poor data management and advised to take precautions to ensure data security. However, many workers are overwhelmed by conflicting administrative priorities, cybersecurity risks go unnoticed.

Introduction:-

Cybersecurity in healthcare refers to the protection of electronic information and digital assets from unauthorized access, use and disclosure. This includes securing sensitive patient data, medical records, and personal information from hackers, cybercriminals, and potentially malicious actors. Cybersecurity events affecting healthcare organizations are making news with increasing frequency, demonstrating their growing impact and scope. We've seen a variety of incidents, from breaches affecting millions of patient records to attacks that led to the closure of hospitals across the country, including at least one Serious violation caused the death of a patient. Most recently, the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, and the Department of Health and Human Services (HHS) issued joint warnings that the healthcare sector is an increased target. ransomware activity.

Cybersecurity challenges in clinical practice in India

1) Data breaches and privacy issues

i) Patient data security: Electronic health records (EHR) containing sensitive patient information are a top target for criminal's network. Breaches can lead to identity theft and unauthorized access to medical history.

ii) Lack of data encryption: Many healthcare organizations do not use adequate encryption measures making patient data vulnerable to interception.

2) Inadequate infrastructure

i) Outdated systems: Many clinics and hospitals use outdated software and hardware, making them more vulnerable to cyber- attacks.

ii) Limited cybersecurity budgets: Healthcare organizations often have limited budgets for IT infrastructure and cybersecurity, prioritizingmedical care. Instead, it's about facilities and services.

Corresponding Author:- Prof (Dr.) Anu Gauba
Address:- Professor, Amity College of NursingAmity University, Gurgaon.

3) Human factors
i) Lack of awareness: Healthcare staff may lack awareness and training in cybersecurity best practices.
ii) Insider threats: Employees with access to sensitiveinformation could accidentally or intentionally compromise data security.

4) Regulatoryand compliance issues
i) Ware Fragmented regulations: India has a fragmented regulatory landscape with varying data protection standards across statesand entities, making it difficult to adequate implementation of cybersecurity

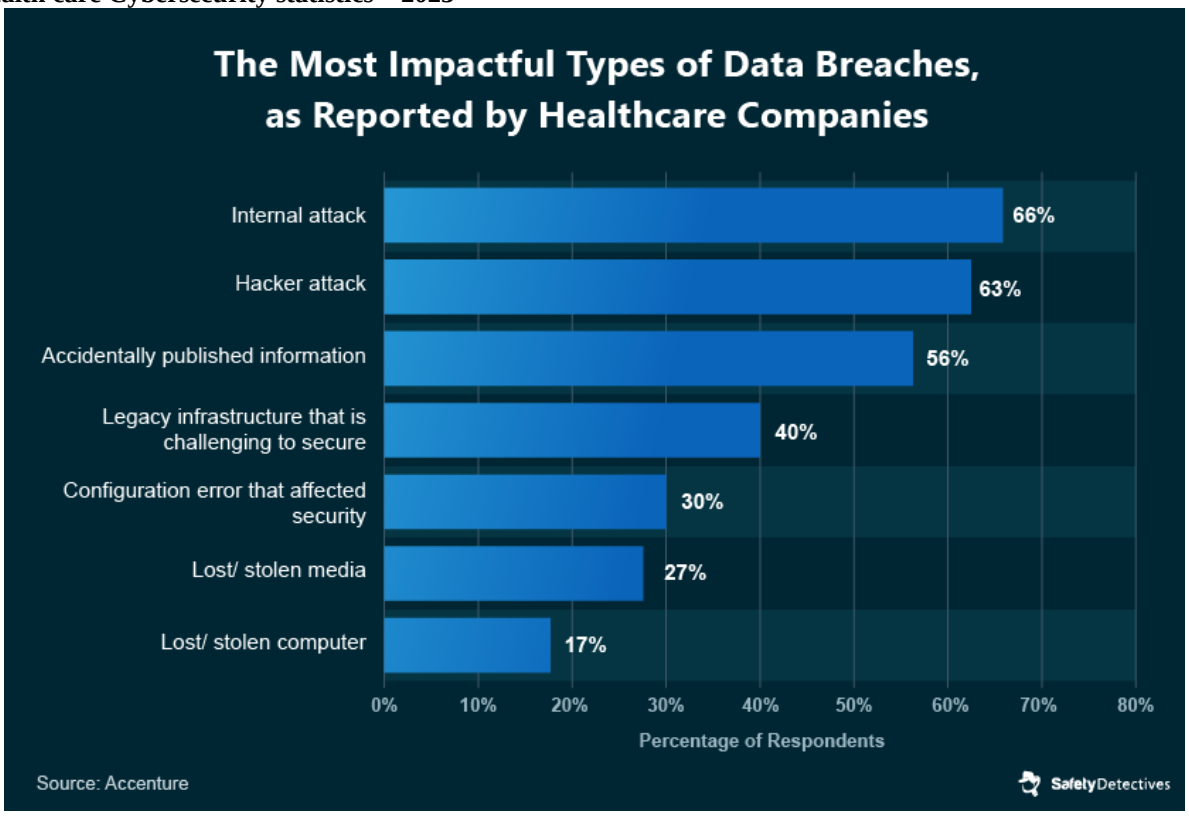
5) Medical Devices and IoT - The growing use of Internet of Things (IoT) devices in healthcare, e.g. connection, can create access points for cyber -attacks 'they are not properly secured.
i) Lack of standardization: Lack of standardized security protocols for medical devices, leading to inconsistent levels of protection.

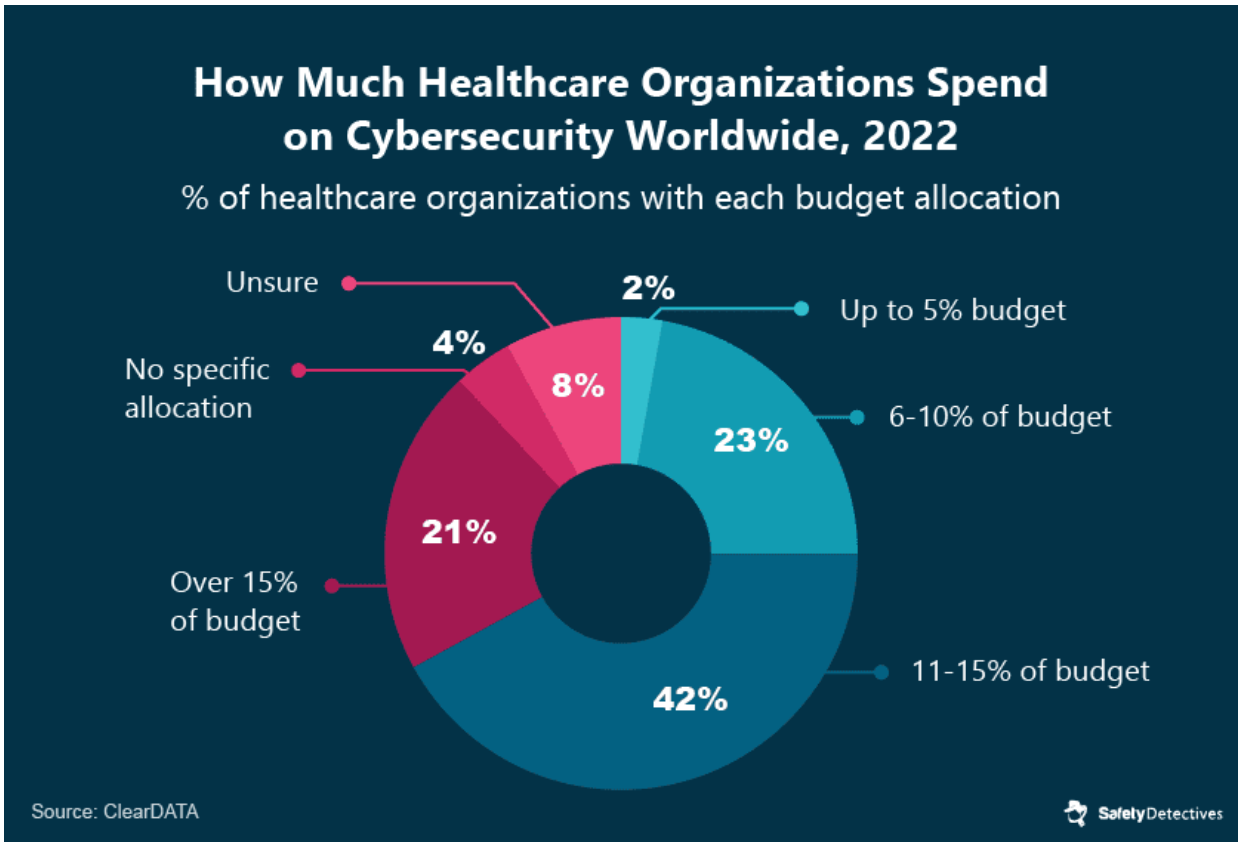
6) Telemedicine and Remote Care:
i) Secure Communication: With the growth oftelemedicine, it is important to ensure secure communication channels for patient consultations. Inadequate security can lead to data leaks and unauthorized access.
ii) Device security: Patients using personal devices for telemedicine consultations may havesecurity measures in place. Incomplete confidentiality, revealing sensitive data.

7)Ransomware and malware attacks - Severe disruption of services: Ransomware attacks can cripple healthcare services by blocking access to critical systems and demanding a ransom for recovery.
i) Cost and resource drain: Recovery from such attacks requires significant resources, both financial and technical, which many healthcare providers may lack.

8) Third-Party Vendors Risk: Many healthcare providers rely on third-party vendors for a variety of services, including IT management. If these vendors have weak security measures, they could become hubs for cyberattacks

Health care Cybersecurity statistics – 2023





Strategies to tackle the challenges

1. Enhance infrastructure: invest in modern and secureIT infrastructure, and ensure regular updates and patches.
2. Staff training: organize regular training on cybersecurity for all medical staff.
3. Regulatory Compliance: Ensure strict compliance with applicable regulations and advocate for more comprehensive and unified cybersecurity legislation.
4. Encryption and access controls: Implement strong encryption measures and strict access controls for patient data.
5. Incident response plan: Develop and regularly update incident response plans to quickly resolve any security breaches
6. Collaboration and collaboration: Collaborate with cybersecurity experts and organizations to stay informed on best practices and emerging threats.

Conclusion:-

In today's electronic world, cybersecurity in healthcare and information protection is essential for the normal functioning of organizations. Many healthcare organizations have different types of specialized hospital information systems, such as EHR systems, electronic prescribing systems, practice management support systems, decision support systems clinical, radiology information system and computerized physician order entry system. Additionally, the thousands of devices that make up the Internet of Things must also be protected. These include smart elevators, smart heating, ventilation, and air conditioning (HVAC) systems, infusion pumps, remote patient monitoring devices, and other devices.

References:-

1. https://www.ncbi.nlm.nih.gov/
2. https://www.hhs.gov/
3. https://www.himss.org/