DISSERTATION REPORT

AT

IIHMR Delhi

A REPORT ON

UNRAVELLING THE ROOT CAUSES OF CYBERATTACKS ON INDIAN HEALTHCARE: A SCOPIC REVIEW

BY

HIMANSHI GOEL

PG/22/038

Under the guidance of

DR. DIVYA AGGARWAL
ASSOCIATE PROFESSOR- HR & OB

PGDM (HOSPITAL AND HEALTH MANAGEMENT)

2022-2024

International Institute of Health Management Research, New Delhi

TO WHOMSOEVER IT MAY CONCERN

This is to certify that **Ms. Himanshi Goel** student of **PGDM (Hospital & Health Management) from International Institute of Health Management Research**, New Delhi has undergone internship training at **IIHMR Delhi** from March 2024 to May 2024.

The Candidate has successfully carried out the study designated to her during internship training and her approach to the study has been sincere, scientific and analytical.

The Internship is in fulfilment of the course requirements.

I wish her all success in all his/her future endeavours.

Dr. Sumesh Kumar
Associate Dean, Academic and Student Affairs
IIHMR, New Delhi

Dr. Divya Aggarwal
Associate Professor, Mentor
IIHMR, New Delhi

Certificate of Approval

The following dissertation titled "Vulnerabilities in The Indian Healthcare System: Unravelling the root causes of Cyberattacks" at "IIHMR Delhi" is hereby approved as a certified study in management carried out and presented in a manner satisfactorily to warrant its acceptance as a prerequisite for the award of **PGDM (Hospital & Health Management)** for which it has been submitted. It is understood that by this approval the undersigned do not necessarily endorse or approve any statement made, opinion expressed, or conclusion drawn therein but approve the dissertation only for the purpose it is submitted.

Dissertation Examination Committee for evaluation of dissertation.

Name	Signature
Dr. Shiv	
Dr. Anandhi	

Certificate from Dissertation Advisory Committee

This is to certify that **Ms. Himanshi Goel**, a graduate student of the PGDM (Hospital & Health Management) has worked under our guidance and supervision. She is submitting this dissertation titled "**Unravelling The Root Causes Of Cyberattacks On Indian Healthcare: A Scopic Review**" at "**IIHMR Delhi**" in partial fulfilment of the requirements for the award of the PGDM (Hospital & Health Management). This dissertation has the requisite standard and to the best of our knowledge no part of it has been reproduced from any other dissertation, monograph, report or book.

Institute Mentor

Dr. Divya Aggarwal
Associate Professor
IIHMR Delhi

INTERNATIONAL INSTITUTE OF HEALTH MANAGEMENT RESEARCH, NEW DELHI

CERTIFICATE BY SCHOLAR

This is to certify that the dissertation titled **Unravelling The Root Causes Of Cyberattacks On Indian Healthcare: A Scopic Review** and submitted by **Himanshi Goel** Enrolment No. **PG/22/038** under the supervision of **Dr. Divya Aggarwal** for award of PGDM (Hospital & Health Management) of the Institute carried out during the period from **March 2024 to May 2024** embodies my original work and has not formed the basis for the award of any degree, diploma associate ship, fellowship, titles in this or any other Institute or other similar institution of higher learning.

Signature

FEEDBACK FORM

Name of the Student: Himanshi Goel

Name of the Organisation in Which Dissertation Has Been Completed: IIHMR Delhi

Area of Dissertation: Cybersecurity in Indian Healthcare Sector

Attendance:

Objectives achieved:

Deliverables:

Strengths:

Suggestions for Improvement:

Suggestions for Institute (course curriculum, industry interaction, placement, alumni):

Signature of the Officer-in-Charge/ Organisation Mentor (Dissertation)

Date:

Place:

INTERNATIONAL INSTITUTE OF HEALTH MANAGEMENT RESEARCH (IIHMR)

Plot No. 3, Sector 18A, Phase- II, Dwarka, New Delhi- 110075

Ph. +91-11-30418900, www.iihmrdelhi.edu.in

CERTIFICATE ON PLAGIARISM CHECK

Name of Student (in block letter)	**Ms. HIMANSHI GOEL**		
Enrollment/Roll No.	PG/22/038	**Batch Year**	2022-2024
Course Specialization (Choose one)	Hospital Management	Health Management	Healthcare IT ✓
Name of Guide/Supervisor	Dr. DIVYA AGGARWAL		
Title of the Dissertation/Summer Assignment	UNRAVELLING THE ROOT CAUSES OF CYBERATTACKS ON INDIAN HEALTHCARE: A SCOPIC REVIEW		
Plagiarism detect software used	"**TURNITIN**"		
Similar contents acceptable (%)	Up to **15** Percent as per policy		
Total words and % of similar contents Identified	11932 TOTAL WORDS 10% SIMILARITY INDEX		
Date of validation (DD/MM/YYYY)	07/07/2024		

Guide/Supervisor

Name: Dr.DIVYA AGGARWAL

Signature:

Student

Name: HIMANSHI GOEL

Signature:

Report checked by

Institute Librarian

Signature:
Date:
Library Seal

Dean (Academics and Student Affairs)

Signature:
Date:
(Seal)

ABSTRACT

At a time when digital technology dominates, the union of cyber security risks and health care system vulnerabilities has become a major global concern. Cyber-attacks have been affecting healthcare centres across the continents, from hacking into databases to highly organized ransom ware infiltration attempts, revealing weaknesses within virtual systems and corrupting patients' confidential information. In this light, India's healthcare industry becomes a centre stage in grappling with surging cyber menaces that undermine not just privacy of medical records but also essential health services. Stepped up adoption of electronic health records (EHRs), telemedicine platforms and networked medical devices has increased the vulnerability of the Indian healthcare system against cyber threats necessitating robust data security measures.

The research paper, "Vulnerabilities in the System: Unravelling the Root Causes of Cyberattacks on Indian Healthcare," delves into the multifaceted nature of cyber threats plaguing the Indian healthcare sector. The study identifies the types and underlying causes of these cyberattacks, emphasizing the critical need for enhanced cybersecurity measures. As healthcare systems increasingly rely on advanced technologies such as artificial intelligence (AI), the complexity of data security challenges also escalates. This abstract encapsulates the discussion on the necessity for AI regulation, adoption of global cybersecurity best practices, and implementation of prevention techniques, ultimately aiming to fortify the healthcare sector's defences against cyber threats.

The research underscores the importance of network segmentation to mitigate the impact of cyberattacks. The lack of proper segmentation in healthcare institutions can lead to a "domino effect," where compromising one part of the network jeopardizes the entire system. The study cites the 2023 AIIMS attack as a case where inadequate network segmentation exacerbated the consequences of the breach. Proper segmentation involves creating sub-networks with distinct security controls to limit the lateral movement of attackers.

In the midst of this background, this research intends to carry out an all-inclusive exploration on cyber threats facing Indian healthcare and their relation with data protection gaps. Based on reviewing scientific research articles, reports by various news media outlets, as well as statistical evidence about cyber-crimes; the study is aimed at clarifying complicated relations underlying attacks by hackers targeting health institutions in India. It is aimed at finding out the root causes of this upsurge in cyber incidents, its impact on the security of patient data and functioning of health care systems and finally recommends measures for making the Indian health care system more resilient to new forms of cyber perils. This study aims at unravelling the multifaceted challenges that come with cyber threats as well as advocating for proactive cybersecurity measures in order to protect the integrity and access to healthcare services in India during this age where everything is done digitally.

ACKNOWLEDGEMENT

I am deeply grateful for the invaluable guidance and support provided by Dr. Divya Aggarwal throughout the course of this dissertation project. Her expertise, insightful feedback, and constant encouragement were instrumental in shaping this work. I sincerely thank her for her unwavering commitment and dedication to my academic growth.

I would also like to extend my appreciation to the faculty and staff of International Institute of Health Management Research (IIHMR) Delhi for creating an enriching academic environment and for providing the necessary resources and support. Special thanks go to my colleagues and friends for their camaraderie and constructive discussions that helped me navigate through various challenges during this project.

I am profoundly thankful to my family for their love, patience, and unwavering support, which gave me the strength to persevere. Their belief in my abilities has been a constant source of motivation.

Lastly, I express my gratitude to all those who contributed directly or indirectly to this dissertation. Your support has been vital in completing this work successfully.

Date: **Himanshi Goel**

Table of contents

List of figures

List of Tables

List of Abbreviations

S.No	Abbreviation	Meaning/Full-form
1	IIHMR	International Institute of Health Management Research
2	CERT-In	The Indian Computer Emergency Response Team
3	HIPAA	The Health Insurance Portability and Accountability Act
4	DISHA	Digital Information Security in Healthcare Act
5	GOI	Government of India
6	AIIMS	All India Institute of Medical Sciences
7	AI	Artificial Intelligence
8	DoS	Denial of Service
9	EHR	Electronic Health Record
10	DDoS	Distributed Denial of Service
11	USA	United States of America
12	GDPR	General Data Protection Regulation
13	APTs	Advancement Persistent Threats
14	IT-Act	Information Technology Act 2000
15	NCRF	National Cybersecurity Response Framework
16	MEITY	The Ministry of Electronic and Information Technology of India
17	SME	Medium–Sized organizations
18	ET	Economic Times
19	NIC	National Informatics Centre
20	DSCM	Database Standards Compliance and Monitoring
21	PHI	Personal Health Information
22	SSL	Secure socket Layer
23	MDP	Management Development Program

ABOUT IIHMR DELHI

The International Institute of Health Management Research (IIHMR), New Delhi is allied to the 'Society for Indian Institute of Health Management Research' which was established in October 1984 under the Societies Registration Act-1958. IIHMR-Delhi was set up in 2008 in response to the growing needs of sustainable management and administration solutions critical to the optimal function of the healthcare sector both in India and in the Asia-Pacific region. We are a leading institute of higher learning that promotes and conducts research in health and hospital management; lends technical expertise to policy analysis and formulation; develops effective strategies and facilitates efficient implementation; enhances human and institutional capacity to build a competent and responsive healthcare sector. Our multi-dimensional approach to capacity building is not limited to academic programs but offers management development programs, knowledge and skills-based training courses, seminars/webinars, workshops, and research studies. Our four core activities are… Academic courses at masters and doctoral level in health and hospital management to meet the growing need of skilled healthcare professionals. Research that has high relevance to health policies and programs at national and global level. Continued education through management development programs and executive programs for working professionals to help them upgrade their knowledge and skills in response to the emerging needs of the industry. Technical consultation to the national and state-level flagship programs to address the gaps in planning as well as implementation.

International Institute of Health Management Research, New Delhi (IIHMR-Delhi)

Over the years IIHMR-Delhi has emerged as an institute of repute both nationally and globally for producing socially conscious, skilled and vibrant top-class health care

management professionals. Our graduates are well-matched for the ever-changing health care sector and evolving social milieu. The institute has progressed as a leader in research, teaching, training, community extension programmes and policy advocacy in the field of health care. IIHMR has carved out a niche for itself through its cutting-edge academic curriculum, infrastructure, accomplished multi-disciplinary faculty and research. The Institute as an autonomous body of international stature has been developing leaders for several years to shape tomorrow's healthcare by equipping the students in the fields of health, hospital, and health information technology. The Institute's dynamic health care research programmes provide rigorous training in management, health systems, hospital administration, health care financing, economics, and information technology.

Commitment to Inclusive Excellence

As an institute, IIHMR-Delhi is committed to creating an environment of higher learning that can serve as the model for the kind of society it strives to build – one of equity, social justice and mutual support. We have also made a concerted effort to promote the ethos and philosophies amongst today's students and nurture them into growing as effective managers, to think both critically and ethically, to learn to cope with ethical dilemmas and apply systems-thinking approaches to serious and complex societal problems. Our internationally renowned faculty lead multidisciplinary health research in multifarious areas such as public health, health services, health economics, hospital management, social determinants of health, mental Health and other topics of global and national interest. The IIHMR is invited by various governmental and civil society organizations to provide technical support for capacity building and policy research needs that culminates in developing innovative and equitable health care strategies and providing advocacy support for health policy and planning. The institute also responds to global health threats, natural disasters, conflict and

related humanitarian crises. In addition to the Masters and doctoral level programmes, IIHMR-D also offers several highly specialized and popular Management Development Programmes (MDP) to a wide range of health professionals in the country and overseas which largely addresses educational needs amongst in-service aspirants.

SECTION 1

Introduction

The digital revolution has transformed healthcare delivery, but with increased reliance on technology comes a new set of vulnerabilities: cyber-attacks. Cyberattacks are any malicious activities carried out through digital channels against computer systems, networks or data. Some forms these attacks may take include but are not limited to malware infections; phishing scams; ransomware; denial-of-service (DoS) attacks among others. Conversely, cyber security entails protecting such digital assets from being harmed by these types of ill-intended acts. The world we live in today is more than ever connected digitally hence many countries suffer greatly when there is an increase in the number and variety of cyber-attacks launched against individuals as well as organizations within them.

For this reason alone, do we need stronger safeguards against cyber threats globally? A priority now should be safeguarding sensitive material alongside critical infrastructure for economies worldwide given that attackers might use weaknesses they find while trying to gain money, gather information or disrupt activities. Nowadays, so much more gets done online than it used to be and so the internet has become a prime hunting ground for criminals looking to make quick dishonest money for themselves at other people's expense.

More often than not they will go after financial institutions like banks where there is large amounts of cash flow happening daily but recently even health care providers have turned into targets because their systems store personal records about patients which could then easily be sold on dark web markets or used by identity thieves who want insurance policies under someone else's name. This can all cause great harm as lives depend on having accurate histories available during treatment; however, if this information falls into wrong hands, then those affected might never get proper medical attention again due lack thereof.

The suggested article's workflow is shown in Figure 1.1. We give an overview of cyberattacks in Section 1 along with information on their types, purposes, problems in the healthcare system, and some initiatives the Indian government has taken in this area. Section 2 presents an overview of the study's purpose and justification. The literature review and technique considerations are introduced in Section 3. A summary of the study's analysed portion is provided in Section 4 along with pertinent tables and figures based on the data gathered. Section 5 addresses the underlying reasons for the various kinds of cyberattacks. A real-world case study is presented in Section 6, and the last section serves as the study's conclusion.

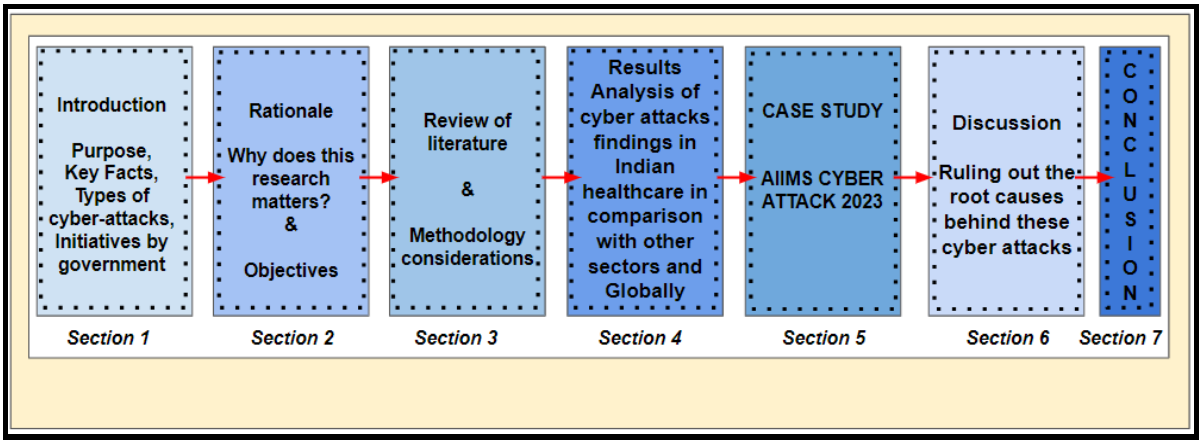

Figure 1.1: Workflow of the study

Cyberattacks and privacy issues

India's healthcare sector is undergoing rapid digitization, with initiatives like e-Hospital and telemedicine gaining traction. Modernization and cybersecurity are two challenges the healthcare industry faces in India. Telemedicine, electronic health records (EHRs), and health information systems have the potential to improve patient outcomes as well as operational efficiency but this also opens doors for attacks from cyberspace because of weaknesses that

come with them. This means that there should be good cyber security measures put in place so that patients' sensitive data is protected while ensuring continuity and reliability of health care services.

Types of Cyber-Attacks

Over the past few years, India has experienced a number of cyberattacks. Data breaches, malware assaults, phishing attempts, ransomware attacks, distributed denial-of-service (DDoS) attacks, insider attacks, etc. are a few of them. Table 1 below describes the various kinds of cyberattacks and includes an actual instance from India as an example.

Type of Attack	Description	Example (real life)	Link
Data Breaches	Unauthorized access compromises sensitive information, such as personal or financial data, through exploitation of vulnerabilities in systems or networks, leading to potential misuse or exposure.	On October 31, 2023, in a massive data breach, information of over 81.5 crore Indians with the ICMR were sold on the dark web.	https://www.financialexpress.com/healthcare/news-healthcare/questions-abound-but-icmr-still-silent-on-the-data-leak/3293107/
Malware Attacks	Malicious software infiltrates systems to disrupt, damage, or gain unauthorized access to data, often through viruses, worms, or trojans.	In August 2018, a malware attack on the Apollo Hospitals Group impacted patient data and caused disruptions to the group's services.	https://icssindia.in/blog/healthcare-sector-is-the-biggest-target-for-cyber-attacks/
Phishing Attacks	Deceptive emails or messages trick users into revealing sensitive information or installing malware by posing as trustworthy entities.	In February 2019, the Indian Health Ministry reported that several government health organizations had been targeted by phishing emails.	https://icssindia.in/blog/healthcare-sector-is-the-biggest-target-for-cyber-attacks/
Distributed Denial-of-Service (DDoS) Attacks	Distributed Denial of Service floods a network or server with traffic, rendering it inaccessible to legitimate users by overwhelming its capacity.	In December 2018, a DDoS attack on the Medical Council of India (MCI) caused disruption to the MCI's services.	https://icssindia.in/blog/healthcare-sector-is-the-biggest-target-for-cyber-attacks/
Ransomware Attacks	Malicious software encrypts files or systems, demanding payment for decryption, often exploiting vulnerabilities or social engineering	Five servers of the All India Institute of Medical Sciences (AIIMS) had been hacked by	https://thewire.in/government/aiims-servers-cyberattack-ransomware-rajya-sabha

	to infiltrate and hold data hostage for financial gain.	ransomware. An estimated 1.3 terabytes of data were encrypted. The hackers had made it impossible for AIIMS to access its own data.	
Insider Attacks	Trusted individuals exploit their access privileges to sabotage, steal, or manipulate data or systems, posing significant threats due to their intimate knowledge of organizational infrastructure and potential for undetected activity.	In January 2018, an insider attack on the Employees' State Insurance Corporation (ESIC) resulted in the theft of patient data.	https://icssindia.in/blog/healthcare-sector-is-the-biggest-target-for-cyber-attacks/

Table 1.1: Types of cyber-attacks with real life cases from India

Worldwide, patient privacy is the most important issue and jurisdiction, and all nations have agreed that protecting people's privacy must be done so at any cost. Humans have the fundamental right to privacy. Privacy policies are rigorously prioritized in several nations, mainly in the USA and Europe. Well-known legislation like GDPR and HIPAA provide individuals confidence in their privacy issues and support them in establishing trust. Significant amounts of unstructured healthcare data are also available in India. Furthermore, due to the problems around data transformation and storage, this may result in privacy violations.

Privacy is not regarded as a critical issue in India. India's distinct healthcare privacy challenges are brought on by infrastructure, politics, culture, and budgetary constraints in addition to a general sense of complacency, etc. Owing to these reasons, data security must take a backseat in order to facilitate quick access to private information (1).

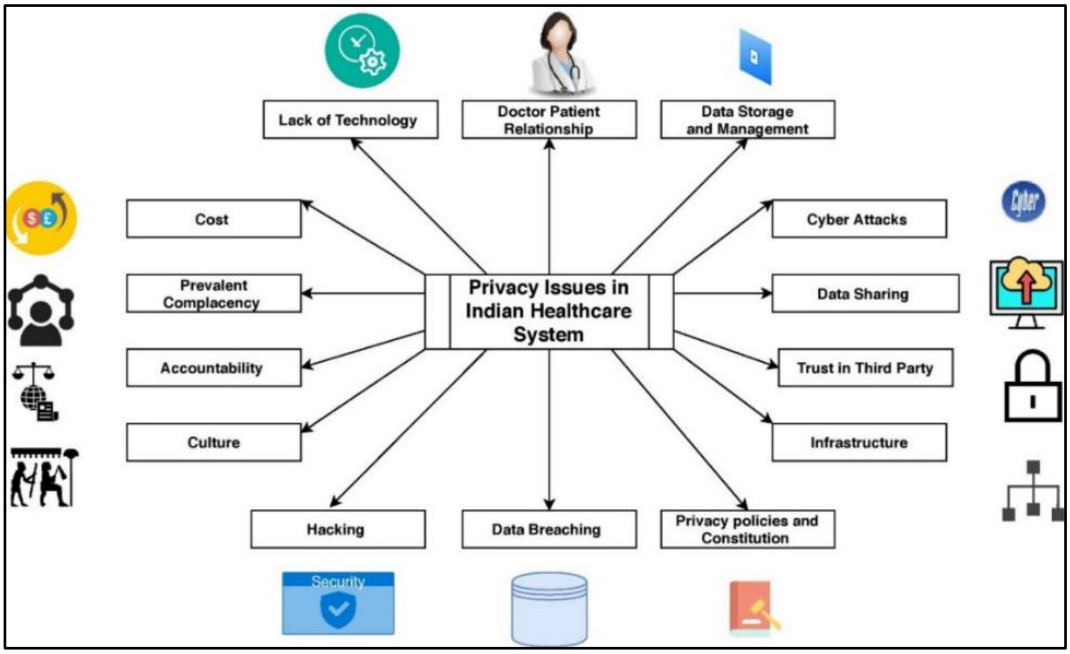

Figure 1.2: Privacy Issues in Indian Healthcare System (1)

Cyberattacks in Healthcare since the Onset of COVID-19 in India

The cyber security challenges in Indian health care were worsened by the COVID-19 pandemic. The criminal hackers found a gold mine with an increased focus on telemedicine and booking appointments online. Reports indicated that phishing scams aimed at vulnerable patients looking for COVID-19 information or test results had surfaced. This added to the fact that institutions conducting vaccine research were also targeted by these malicious actors. Healthcare providers were under great pressure during this time which might have resulted in relaxation of security protocols thereby increasing the attack surface even more. This period brought out clearly the need for strong cyber defence measures within the health sector.

In India, at the start of COVID-19 pandemic, there was a rush among organizations to adopt digital solutions for managing patient care and administrative processes remotely because of

which it has further intensified the cyber security risks associated with the healthcare industry. Although this fast transformation is crucial in ensuring continuity of services during emergencies but it has also exposed different weaknesses within our systems making them open to cyber-attacks as such systems are easily infiltrated by criminals who take advantage when they find any gap in such defences which were meant only for protecting against normal threats but not those posed by advanced persistent threats (APTs).

This study investigates several cybersecurity concerns, issues, and difficulties that arose since the COVID-19 outbreak. Nonetheless, several categories of cybersecurity issues were recognized, which were prevalent amid the COVID-19 outbreak (5). The most prevalent cyberattack kinds were found to be ten in number: Malware, phishing, ransomware, distributed denial-of-service (DDoS), malicious domains, botnet attacks, hacking, spam emails, malicious messages, and APT.

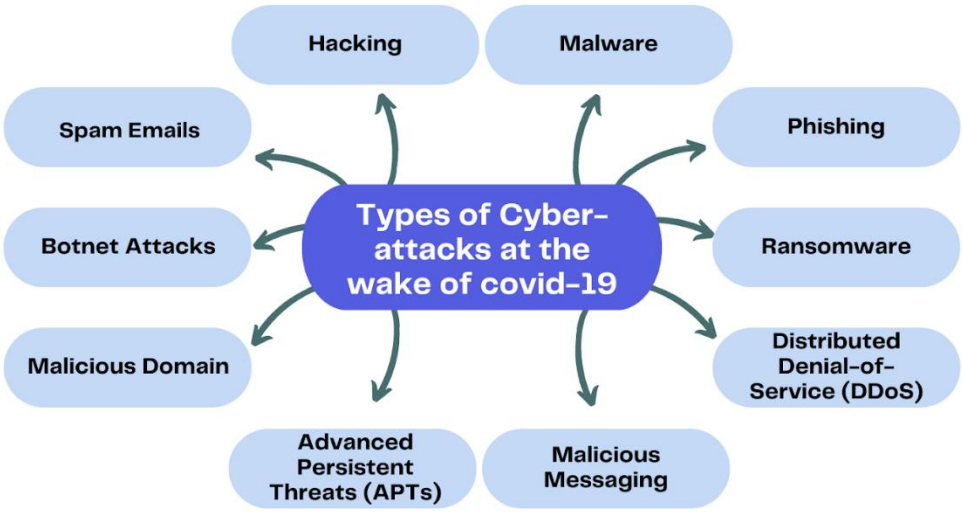

Figure 1.3: Types of cyber-attacks at the wake of covid-19 (5)

Initiative taken by GOI for cyber security

To respond to increasing threats against its cyber space, the Indian Government has taken steps aimed at making national infrastructure resilient enough before any risks can manifest themselves into realities.

Table 2 explains a few initiatives taken by the Government of India in the context of maintaining cyber security in our country, such as, IT Act 2000, establishment of CERT-In team, National Cyber Security Strategy, etc.

Legislation/Policy	Description	Applicability to Healthcare
Information Technology Act, 2000 (IT Act)	The primary law governing cybercrime and electronic commerce in India. Defines cyber offenses like hacking, data theft, and prescribes penalties.	Yes. The IT Act applies to all forms of electronic transactions, including those in healthcare. Provisions like data security and privacy are particularly relevant.
National Cyber Security Strategy (2013)	A high-level document outlining the government's vision for a secure cyberspace in India.	Yes. The strategy emphasizes protecting critical infrastructure, which includes healthcare.
CERT-In (Indian Computer Emergency Response Team)	A government body under the Ministry of Electronics and Information Technology (MeitY). It is responsible for handling cyber security threats and vulnerabilities.	Yes. CERT-In plays a crucial role in responding to cyber incidents in healthcare institutions. It issues advisories and coordinates with healthcare providers during attacks.
DISHA (Digital Information Security in Healthcare Act)	Not enacted yet. A proposed legislation that aims to specifically address cyber security in the healthcare sector.	Yes. If enacted, DISHA would establish a robust framework for data security and privacy in healthcare institutions.
National Cybersecurity Response Framework (NCRF)	A framework under development to provide a standardized approach for critical infrastructure sectors, including healthcare, to respond to cyber incidents.	Yes. NCRF will provide healthcare institutions with guidelines for incident response, recovery, and mitigation strategies.

Table 1.2: Initiative taken by GOI for cyber security

It is important for us not only to know but also appreciate that the sophistication levels plus size complexities surrounding threats posed by hackers keep changing daily hence we must remain ever vigilant by adopting appropriate countermeasures lest our institutions compromise their own credibility through breaches arising out of lack thereof. While these steps taken are laudable there need be more done if they are to succeed fully; such an approach calls necessarily upon investing heavily into secure foundations besides creating awareness among staff members within hospitals on how best deal with such issues whenever they arise even as we engage experts who can assist us overcome this challenge together as a nation. Only through a multi-pronged strategy can India's healthcare sector embrace the digital future while safeguarding the privacy and security of its patients.

SECTION-2

RATIONALE

The healthcare industry in India is experiencing a rapid digital shift where patient information is increasingly stored and transmitted electronically. There are several advantages to doing this such as efficiency improvements and care accessibility enhancements, but also a number of new cybersecurity problems that come with it. Institutions handling sensitive data have become major targets for cyberattacks.

The purpose of this research project is to examine the weaknesses in the Indian healthcare information systems and identify the underlying reasons why this industry is the target of cyberattacks. We might improve cyber security in Indian healthcare and safeguard patient data by creating efficient mitigation solutions by comprehending these vulnerabilities and their underlying causes.

Why Does This Research Matters?

- Increasing Cyber Attacks: The risk of falling victim to cyber-attacks keeps growing in Indian healthcare systems. Over the years there has been an exponential increase in the number of cyber-attacks against health facilities within India thus there's need to find out what are some common grounds or factors leading up-to these incidents so as to prevent future recurrence.

- Vulnerable Data: These attacks compromise private patient records. Healthcare data contains personal details together with medical history thus any breach may result into identity theft which in turn leads to financial loss not only for individuals but also

hospitals involved since they'll be held liable under law enforcement agencies for their negligence towards safeguarding other people's lives.

- Disrupted Patient Care: Cyberattacks can disrupt access to patient data and medical records, potentially delaying critical care and impacting patient outcomes.

- Reputational Damage: Successful cyberattacks can damage the reputation of healthcare institutions, eroding patient trust and impacting their ability to deliver quality care.

OBJECTIVES OF THE STUDY

1. To analyze the recent trends and patterns of cyberattacks on Indian healthcare institutions from previously published literature.

2. To identify the vulnerabilities within Indian healthcare systems that render them susceptible to cyber threats as per literature available.

3. To suggest effective countermeasures on effective weak points in the Indian Healthcare system as published by GOI.

SECTION 3

Review of Literature

A study emphasizes the critical role of cybersecurity education for healthcare professionals. Their study, conducted in the UK, underscores the need for national educators, global organizations, and policymakers to integrate comprehensive cybersecurity training into healthcare education. This approach aims to mitigate the permanent and substantial threat posed by cyber-attacks to health systems by enhancing the cybersecurity awareness and skills of healthcare practitioners.(64)

A detailed study provides analysis of various types of data breaches in healthcare organizations. Conducted in the USA, the study reveals the nature of healthcare data breaches, examining their impact on data confidentiality, security, and cost-effectiveness. The authors also explore forecasting methods for predicting data breaches, highlighting the importance of proactive measures to safeguard healthcare data.(14)

This study represents a comprehensive survey on the evolution, concerns, and security challenges of the Internet of Things (IoT) in healthcare. Based in India, their research outlines various types of attacks and abnormalities associated with IoT devices and offers insights into identifying and mitigating these threats. The study highlights the significance of robust security measures for IoT systems to prevent cyber-attacks in healthcare.(16)

The study focuses on the architecture and security challenges of the Internet of Medical Vehicles (IoMV). The research, set in India, discusses the system concept of IoMV and identifies key cybersecurity risks. It suggests that addressing these challenges is crucial for securing the rapidly advancing field of connected medical vehicles and ensuring safe and reliable healthcare delivery.(11)

Sathish Kumar Chintala (2022) examines data privacy and security challenges in AI-driven healthcare systems in India. The study explores governmental regulations, such as the National Medical Commission Act and Telemedicine Practice Guidelines, addressing

legal issues related to health data. It emphasizes the need for stringent cybersecurity measures to protect sensitive health information in the context of AI technologies.(13)

The COVID-19 pandemic significantly altered the landscape of cybersecurity in the Indian healthcare sector. According to a study by Express Healthcare (2023), the pandemic led to a notable increase in cyber-attacks. This study analyses how the surge in remote healthcare services and telemedicine during the pandemic heightened vulnerabilities and necessitated enhanced cybersecurity measures.(65)

A subsequent study outlines various strategies for securing cybersecurity in healthcare, including implementing information security governance, enforcing hygiene, and adopting multi-factor authentication. These strategies aim to address new and emerging threat surfaces, emphasizing proactive measures to manage detection and response to cyber threats.(19)

This study explores the use of Cyber-Physical Systems (CPS) and AI strategies for detecting cyber-attacks in healthcare. The study discusses how AI algorithms can predict cyber-attack patterns and aid in decision-making for medical professionals. By leveraging Smart Healthcare Cyber-Physical Systems (SHCPS), healthcare organizations can enhance their capability to identify and respond to cyber threats.(10)

Research provides a comparative study on privacy and security concerns in Electronic Health Records (EHR) between India and the USA. Their research highlights gaps in India's current regulations and suggests reforms to address these challenges. The study offers valuable insights into improving EHR security and privacy, crucial for protecting patient data in both countries.(1)

By conducting a SWOT analysis to address data security and privacy issues in the healthcare sector, this study identifies strengths, weaknesses, opportunities, and threats

related to healthcare data security, offering strategic recommendations for overcoming cybersecurity challenges and enhancing data protection.(21)

This study examines contemporary cybersecurity trends in health information systems. The research highlights prevalent cyber threats, such as ransomware and denial-of-service attacks, and discusses their applicability to health information systems. The study underscores the need for ongoing vigilance and adaptation to evolving cyber threats.(4)

A survey for the cybersecurity issues that emerged during the global COVID-19 crisis has been conducted. The study identifies the most common forms of cyber-attacks during the pandemic and examines their catastrophic outcomes. This analysis helps in understanding the vulnerabilities exposed by the pandemic and the measures needed to mitigate future risks.(8)

A systematic study on the quantitative examination of cybercrime during the COVID-19 pandemic was done in India. The study investigates the social impact of cybercrime and outlines effective countermeasures to mitigate these challenges. Their findings reveal a significant increase in cyberattacks, including phishing and ransomware, during the pandemic, attributing this rise to the rapid digital transformation and increased reliance on online platforms for healthcare services.(7)

By a comparative analysis, the study explores privacy and security concerns related to Electronic Health Records (EHR) in India and the USA. This study identifies gaps in India's current and proposed regulations and contrasts them with the regulatory landscape in the USA. The authors emphasize the need for comprehensive policy reforms to enhance the security and privacy of EHR systems in India, highlighting critical areas such as data encryption, access controls, and compliance with international standards.(20)

Using a SWOT analysis to examine the challenges of data security and privacy in the healthcare sector globally. Their study identifies strengths, weaknesses, opportunities, and

threats related to healthcare data security. They offer strategic recommendations, such as adopting advanced encryption technologies, implementing stringent access control measures, and promoting cybersecurity awareness among healthcare professionals.(3)

This study focuses on contemporary cybersecurity trends in health information systems. This global study highlights prevalent cyber threats, including ransomware and denial-of-service attacks, and discusses their implications for health information systems. The authors advocate for continuous adaptation to evolving cyber threats, emphasizing the need for robust cybersecurity frameworks and regular security assessments.(12)

A study presents a survey of cybersecurity issues that emerged during the global COVID-19 crisis. The study identifies fifteen prevalent forms of cyberattacks, including phishing, malware, and denial-of-service attacks. The authors analyse the catastrophic outcomes of these attacks and suggest measures for improving organizational cybersecurity resilience, such as enhancing incident response capabilities and implementing multi-layered security strategies.(5)

METHODOLOGY

The study design would be a descriptive secondary research and analysis. The aim is to comprehensively understand the trends, vulnerabilities, and root causes of cyberattacks on the Indian healthcare sector over the specified timeframe.

Research Question

What are the root causes of the increasing cyberattacking on the Indian Healthcare sector, especially since the covid-19 outbreak?

Research Design

The study will involve a comprehensive literature review and analysis. This involves gathering, synthesizing, and critically evaluating existing scholarly articles, news articles, statistical reports, and annual reports from authoritative sources like CERT-In.

Data Type: Literature-based Secondary data

- Scholarly articles from PubMed and Google Scholar (17 articles were studied in detail after applying inclusion and exclusion criteria that has been mentioned below).
- News articles from reputable sources covering cyberattacks on Indian healthcare (approx. 20).
- Statistical reports on cybercrime in India from credible sources (approx. 25).
- CERT-In annual reports detailing cyber incidents and vulnerabilities in various sectors including health care.

Study Area

The study focuses on cyber-attacks on the health care sector in India including incidents, vulnerabilities and preventive measures within this domain.

Study duration

March 2024 - May 2024

Data Collection Methods

- Literature Search: Secondary research and retrieval of scholarly articles from PubMed and Google Scholar using relevant keywords and search strings (17 articles were studied in detailed manner).
- News Aggregation: Collection of news articles from reputable sources reporting on cyberattacks targeting Indian healthcare institutions.
- Statistical Reports: Retrieval of statistical reports on cybercrime in India from authoritative sources such as Statista, financial express, etc.
- CERT-In annual reports: Retrieval of reports published by CERT-In, which tells us about how many cyber cases were handled by Indian Computer Emergency Response Team (CERT-In) and Ministry of Electronics & Information Technology (MeitY).

Keywords: Cyberattacks, healthcare, India, cybersecurity, vulnerabilities, data breaches, patient privacy, preventive measures, root causes, statistical reports, CERT-In, systematic review, ransomware, phishing, malware attacks, etc.

Data Analysis

This type of analysis has been categorized into three:

- Thematic analysis: identifying trends, patterns and recurring themes from the literature collection.
- Comparative analysis: comparing findings or results by different sources in terms of the evolution of cyber threats, vulnerabilities and mitigation strategies for Indian healthcare.
- Synthesis: integrating findings so as to provide a relation on how key challenges in the cyber threat landscape in the Indian healthcare sector can be addressed.

Study Population

Inclusion Criteria:

These are cybersecurity articles which address cyber-attacks against the Indian health care department either by scholarly articles, news articles or reports.

Some statistical reports and annual reports from reputable sources like government agencies including cybersecurity organizations.

Exclusion Criteria:

In this case, we were interested only in studies associated with cyber-attacks on Indian health care system.

Such materials as reports or articles that do not have credibility concerning the study topic were ignored.

SECTION 4

RESULT(Findings)

The comprehensive analysis conducted on the vulnerabilities within the Indian healthcare system has pinpointed a critical root cause: improper network segmentation as discussed further in the study. These finding aligns with global trends, indicating that inadequate network segmentation is a pervasive issue contributing significantly to cybersecurity breaches in healthcare systems worldwide.

In addition, it is important that government agencies, healthcare providers and cyber-security experts work together to formulate and enforce strict rules, regulations and instructions that are meant to address challenges specific to this sector. Through promoting a culture of awareness on cyber security resilience in the country as well as across the globe, India stands a better chance of reducing the dangers associated with poor network segregation while protecting patient information systems and overall safety against online hackers.

4.A Thematic Analysis

This part contains thematic analysis that pulls trends, patterns and repeating thoughts from collected previously published literature on cyber security in Indian health care system by showcasing the trends since the covid-19 outbreak in the country.

4.1 Cybersecurity Trend in India and Globally

179 million Indian Rupees!

That's the average cost of data breach in India 2023(26). A record high for the report and an almost 28% rise from 2020. Costs associated with detection and escalation increased by 45% during this same period, accounting for the largest share of breach expenses and suggesting a move toward more intricate breach investigations.

The below table 4.1 represents the percentage of the cyber-attacks happening in different countries. It has been clearly represented that India has become one of the most targeted countries worldwide, accounting for 13.7% of all cyberattacks. With 9.6% of all attacks, the United States is the second most attacked nation. China and Indonesia come next, accounting for 4.5% and 9.3% of all attacks, respectively.

Country	Portion of cyber attacks
Other	62.90%
India	13.70%
US	9.60%
Indonesia	9.30%
China	4.50%

Table 4.1: Percentage of cyberattacks across different countries (43)

According to the 2023 India Threat Landscape Report by Singapore-based cybersecurity company Cyfirma, targeted cyberattacks on government institutions increased by 460% during this time, while those against startups and small and medium-sized organizations (SMEs) increased by 508%. (43)

The information shown in the table was taken from the Cyfirmia report and has been shown graphically in Figure 4.1 for better understanding. Data breaches continue to occur despite improvements in digital infrastructure, presenting serious risks to public and private institutions alike. It is an enormous effort to protect the data of millions of people and consumers. (33)

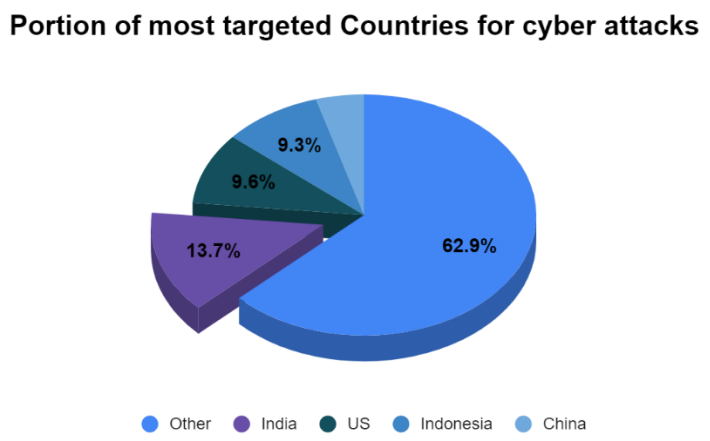

Figure 4.1: Portion of the most targeted countries for cyber-attacks (33)

As India moves forward with its ambitions to digitize all areas of the economy, a widespread cyberattack outbreak has cost businesses a significant amount of money. Because of the complexity of cyberthreats and the growing financial consequences of data breaches, cybersecurity has become a top priority for board members(27).

4.2 Global Trends: Cyber Attacks Targeting Healthcare Sectors Worldwide

According to a Sophos report shared exclusively with ET, about 60% of healthcare businesses worldwide experienced a cyberattack in the previous 12 months, making the healthcare industry a prime target for hackers. (30)

Of these, in around 75% of ransomware operations, thieves were successful in encrypting data. According to the UK-based cybersecurity company, this is a considerable increase from the 61% of data encryptions carried out last year and the greatest percentage of encryption in the previous three years. (30)

Industries	Share of cyber-attacks
Manufacturing	25.70%
Finance and insurance	18.20%
Professional, business, and consumer services	15.40%
Energy	11.10%
Retail and wholesale	10.70%
Healthcare	6.20%
Government	4.30%
Transportation	4.30%
Education	2.80%
Media and telecom	1.20%

Table 4.2: Share of cyberattacks across different industries globally (30)

Table 4.2 represents the share of cyber-attacks across various industries such as, Manufacturing, finance, Customer services, healthcare, retail, transportation, etc. globally in 2023.

It can be clearly seen in figure 4.2, the healthcare industry is the sixth most vulnerable to cyberattacks worldwide, accounting for 6.20% of all cyberattacks in 2023. This industry is growing increasingly vulnerable to these attacks. (30)

According to the Sophos report, recovery times for healthcare organizations have increased, with 47% of them recovering in less than a week as opposed to 54% the previous year. (44)

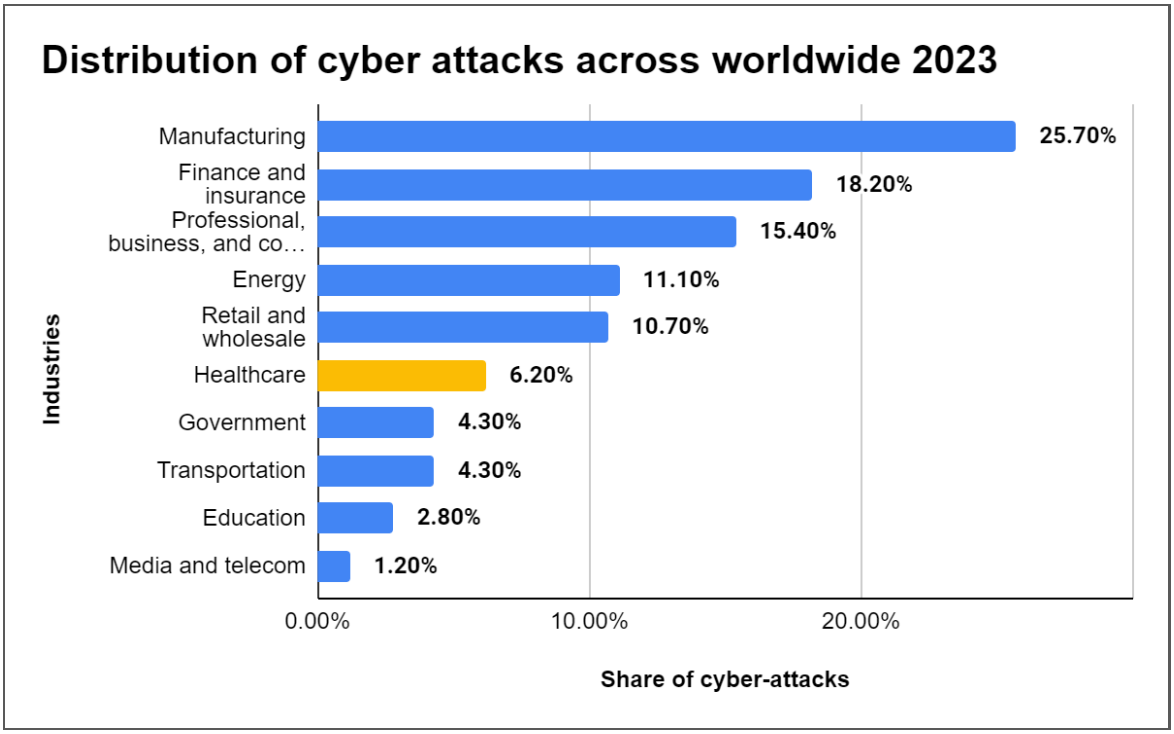

Figure 4.2: Distribution of cyber-attacks across worldwide 2023(30)

4.B Comparative Analysis

In this section we compare different sources on cyber threats, vulnerabilities and mitigation strategies in Indian healthcare sector. This involves bringing together different points of view and using contrasting data sets such as CERT-In (Indian Computer Emergency Response Team) to show years' evolution of the hackers' attacks, identify common vulnerabilities like wrong classification of networks and contrasting effectiveness various measures aimed at protection against new types of threats.

4.3 Cyber Threat Landscape in India: Insights from CERT-In Data

CERT-In (Indian Computer Emergency Response Team)

The Ministry of Electronics and Information Technology, Government of India, operates CERT-In, a functional organization whose goal is to secure Indian cyberspace. In addition to providing security quality management services, CERT-In offers incident prevention and response services.

CERT-In Data	Total Incidents	cyber threats and vulnerabilities		
		Security alerts	Advisories	Vulnerability Notes
2019	394499	204	38	202
2020	1158208	496	93	450
2021	1402809	618	52	390
2022	1391457	653	38	488

Table 4.31: CERT-In data on total number of cyber incidents 2019-2022 (42)

The data in tale 4.3, is collected from the CERT-In annual reports published on their official website. This table represents the total number of cyber incidents that happened during the course of the year 2019-2022, along with the incidents of security alerts, advisories, and vulnerability notes.

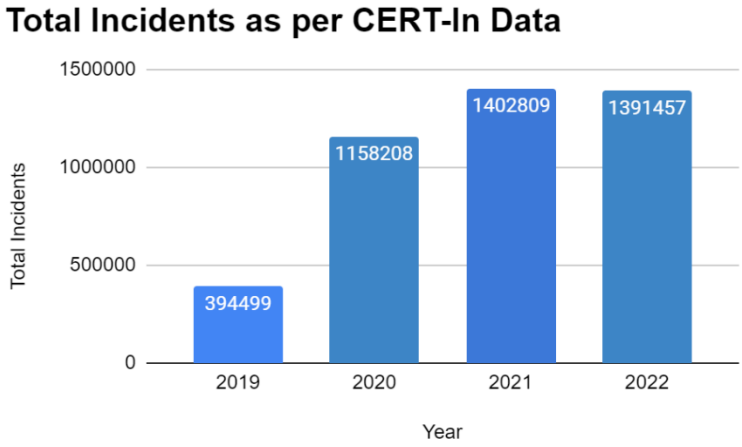

Figure 4.31: Total incidents as per CERT-IN Data (42)

Figure 4.3 makes it evident that the year 2021—shortly after the covid pandemic reached India—saw the highest number of cyber events. (42)

During the pandemic, telemedicine ended up being the only way to get medical attention. Hackers now have an easier time obtaining the necessary data from individual patients because of the treatment. Investigations by law enforcement agencies have shown that most attackers were fairly accurate in estimating the maximum ransom they could seek from the companies they attacked. Thus, according to the FBI Internet Crime Complaint Center,

consumer victims reported total losses from cybercrime of $4.2 billion in 2020, up 69 percent from 2019. (5)

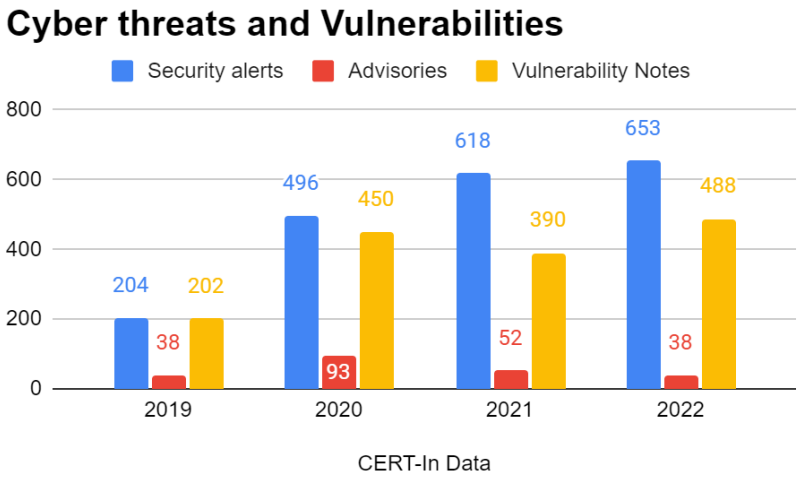

Figure 4.32: Number of cyber threats and vulnerabilities during 2019-2022 (42)

Figure 4.32 sheds light on the number of cyber threats and vulnerabilities happened during 2019-2022, along with specifying the number of security alerts issued, advisories published and vulnerability notes published as reported by CERT-In.

Security Incidents	2019	2020	2021	2022
Phishing	472	280	523	1714
Unauthorized Network Scanning/Probing /Vulnerable Services	305276	1028881	1160333	1200512
Virus/ Malicious Code	62163	99986	209110	161757
Website Defacements	24351	25969	27408	19793
Website Intrusion & Malware Propagation	417	152	1489	2164
Others	1820	2940	3946	5517

Table 4.32: Summary of various types of incidents handled 2019-2022 (42)

Security Incidents	Percentage of Incidents
Phishing	0.1%
Unauthorized Network Scanning/Probing /Vulnerable Services	85%
Virus/ Malicious Code	12.3%
Website Defacements	2.2%
Website Intrusion & Malware Propagation	0.1%
Others	0.3%

Table 4.33: Percentage of total security incidents published by CERT-In (42)

Table 4.32 shows the summary of security incidents reported by CERT-In during 2019-2022 such as phishing. Unauthorized network scanning, malicious code, website defacements, etc. Whereas table 4.33 represents the average percentage for these incidents during 2019-2022.

Figure 4.33 makes it evident that, out of all the incidents that occurred between 2019 and 2022, the most common ones involved unauthorized network scanning, probing, and vulnerable services. These incidents accounted for 85% of all incidents. It may be observed that the majority of mishaps occur as a result of inadequate network security.

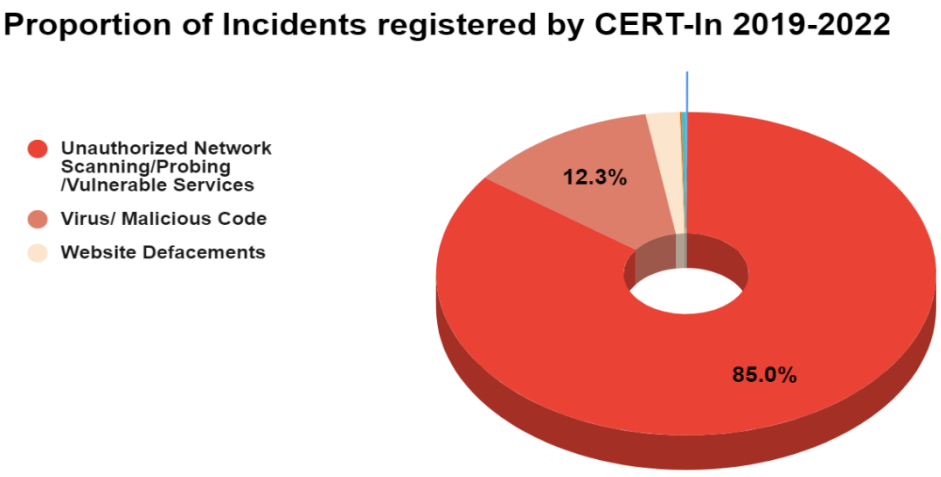

Figure 4.33: Proportion of Incidents registered by CERT-In (42)

4.4 Sector-Specific Analysis: Comparing Cyber Attacks Across Industries in India

India, home to the second-highest number of internet users globally, was not an anomaly to the expanding digital community. Increased internet connectivity offers significant advancements, but it also exposes our digital societies to new threats. Cybercrimes are transnational in nature and have developed in step with new technological advancements (59).

Securing online systems is becoming essential as India progresses with its healthcare digitization. In the previous year, over 60% of Indian healthcare businesses experienced cyberattacks(27).

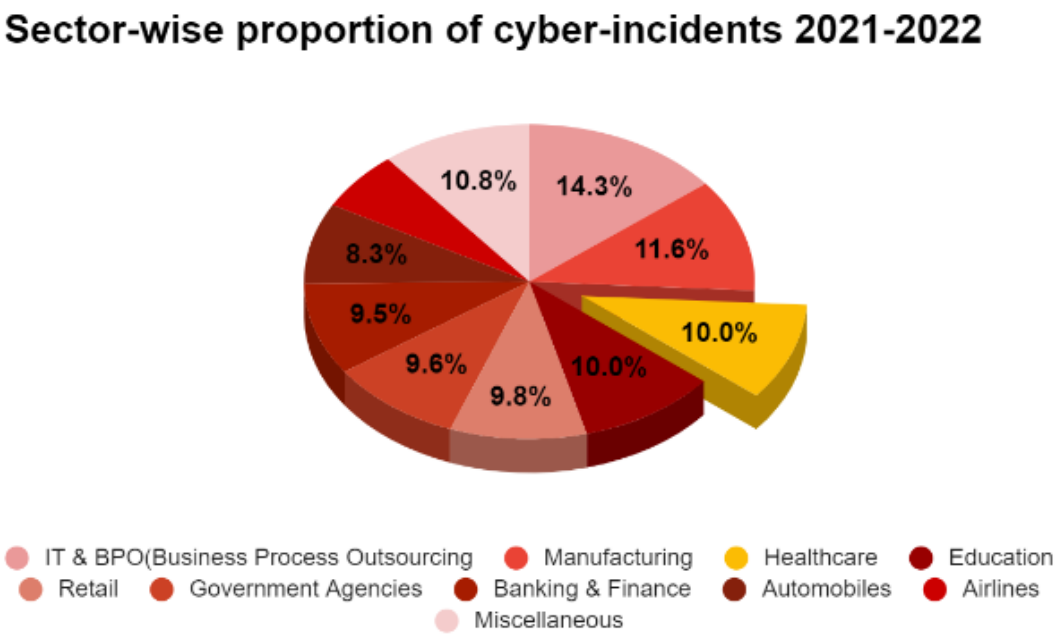

Figure 4.4: Sector wise proportion of cyber incidents 2021-2022

Cyfirma discovered that (table 4.4), in India, 14.3% of cyberattacks targeted service providers, such as IT and BPO. Manufacturing came next, at 11.6%, and healthcare and education came next, at about 10% apiece. Government agencies experienced 9.6% of

attacks, while retail, including online platforms, saw 9.8%. Airlines, cars, and banking and financial services organizations saw 9.5%, 8.3%, and 6.1% of attacks, respectively. (43)

Name of Sector	Number of cyber incidents in 2021-2022	
	Number of incidents	Percentage (%)
IT & BPO(Business Process Outsourcing	399580.038	14.3
Manufacturing	324134.856	11.6
Healthcare	279426.6	10
Education	279426.6	10
Retail	273838.068	9.8
Government Agencies	268249.536	9.6
Banking & Finance	265455.27	9.5
Automobiles	231924.078	8.3
Airlines	170450.226	6.1
Miscellaneous	301780.728	10.8

Table 4.4: Number of cyber incidents in India sector wise

Table 4.4 makes it evident how many cyber incidents occurred in a variety of industries, including retail, healthcare, IT, and so on. (42) Additionally, Figure 4.4 makes it apparent that the healthcare industry in India ranks third most vulnerable to cyberattacks.

According to the Healthcare Cybersecurity Statistics provided, the number of healthcare data fraud cases has increased by almost 400%. Roughly 25% of healthcare workers lack sufficient cybersecurity training, which accounts for 90% of hacks using email phishing. Less

than half of the workforce is incompetent in keeping the sensitive data of the company secure and ineffective in balancing the security budget because they are ignorant of the security measures that have been implemented in their company(14).

4.C: Synthesis

This section talks about the combined findings and how key challenges facing India's health sector can be addressed. It links weaknesses, attack profiles and current countermeasures into a holistic framework for designing effective cybersecurity protocols specific to the unique needs/requirements of health care in India.

4.5 Weak points in Indian Healthcare system with respect to cybersecurity as per NDHM Blueprint

The Government of India (GOI) and the National Digital Health Mission (NDHM) Blueprint have identified several weak points in the Indian healthcare system's cybersecurity posture(66). This section proposes targeted countermeasures to address these vulnerabilities and strengthen cyber defenses.

Weak points

- Outdated IT Infrastructure
- Improper Network Segmentation
- Limited Awareness and Training
- Weak Cybersecurity Culture
- Inadequate Legal Framework

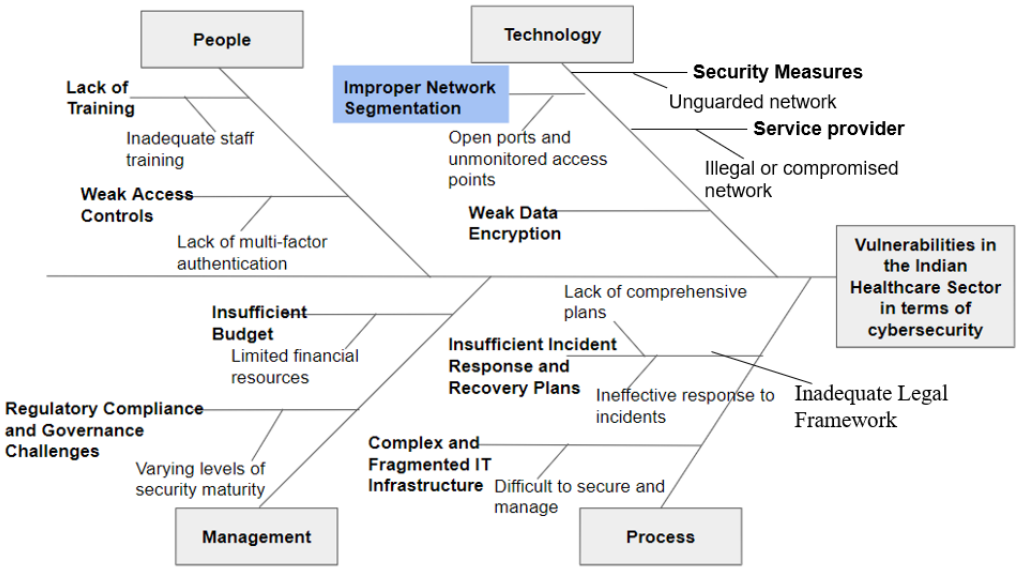

Figure 4.5: Root cause analysis for Indian Healthcare system with respect to Cybercrimes

4.6 Cybersecurity Incidents in Focus: Patterns of Attacks within the Healthcare Industry

Cyberattacks on vital healthcare facilities highlight the harm that inadequate security measures may do to people's lives. Vulnerabilities can be used to terrible effect, especially in industries like energy, banking, electric vehicles, and government databases.

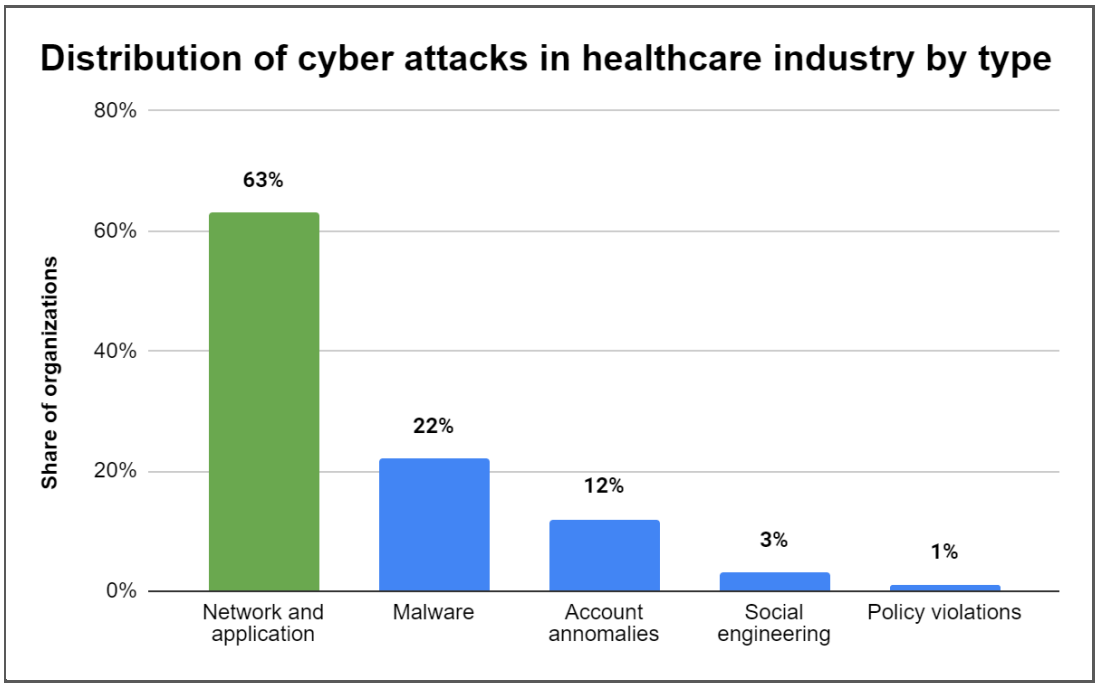

Figure 4.6: Distribution if cyber-attacks in healthcare industry by type

One of the industry's most susceptible to cybercrime is the healthcare sector. The companies in this industry saw a range of cyberattacks, with network and application anomalies accounting for about 63% of the total.(23) Targeting 22% of the firms under examination, malware emerged as the second most prevalent form of attack vector (Figure 4.7).

It is incredibly easy to move laterally within a network without network segmentation. By dividing the network, network segmentation stops this lateral movement and, consequently, access to sensitive data. That essentially set up several security perimeters within the network, as opposed to one security perimeter surrounding the entire network.(61)

4.7 Regulatory Framework: Government Mandates for Cybersecurity Compliance in India

Governments around the world, particularly in industrialized nations, have passed legislation to reduce the threat of data breaches, particularly in the healthcare industry. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 states that improper handling or violation of a patient's right to privacy in the United States is punishable by law. Similar to this, Australia's Information Privacy Act was implemented in 2009 to prevent the disclosure of private information. While New Zealand's Health Information Privacy Code has been in effect since 1994, Canada's Personal Health Information Protection Act went into effect in 2004. (21)

The Digital Information Security in Healthcare Act (DISHA) was created in India in 2019 with the goal of establishing security and privacy safeguards for electronic health data as well as governing its interchange and storage. (21)

Country	Law	Description	Year
United States	Federal Information Security Management Act (FISMA)	Requires federal agencies to develop and maintain a comprehensive information security program.	2002
	Health Insurance Portability and Accountability Act (HIPAA)	Protects sensitive patient data in the healthcare industry.	1996
India	Information Technology Act (IT Act)	Defines cybercrimes and prescribes penalties. May need revisions for the healthcare sector.	2000
	Digital Information Security in Healthcare Act (DISHA)	Proposed legislation specifically addressing cyber security in the healthcare sector (not yet enacted).	-
	Personal Data Protection Bill (PDP Bill)	Upcoming legislation regulating the collection, storage, and use of personal data, including healthcare data.	-
Australia	Cybersecurity Act	Establishes a framework for protecting government and critical infrastructure from cyber-attacks.	2008
New Zealand	Cybersecurity Act	Focuses on information sharing and collaboration between government and industry to improve cyber resilience.	2008
France	Network and Information Security Act (LMSI)	Requires operators of essential services to implement security measures and report cyber incidents.	2004
Singapore	Cybersecurity Act	Comprehensive framework addressing cyber risks, including critical infrastructure protection, data breach notification, and computer misuse offenses.	2018
Germany	Information Security Act (BSIG)	Sets out requirements for the protection of information technology systems operated by critical infrastructure providers.	2016
Japan	Act on the Protection of Information Assets	Aims to protect information assets important to national security and public safety.	2016

Table 4.7: Cybersecurity laws in various countries

Table 4.5 lists the numerous cybersecurity laws that have been passed by various countries, including the US's HIPAA, the Indian government's Personal Data Protection Bill (which is

now being considered but not yet passed), the German Information Security Act, the Singapore Cybersecurity Act, and others.

The government of India has already taken a few steps, as indicated in tables 4.5 and table 1.2, but more has to be done to safeguard the health information system so that the vulnerability to cyberattacks declines quickly. The cybersecurity environment for Indian Healthcare systems is expected to drastically change as a result of the DISHA act.

4.8 Financial Commitment: Government Budget Allocation for Cybersecurity Measures in India (2023)

The Ministry of Electronic and Information Technology of India (MEITY) was purportedly given around six billion Indian rupees for the development of cybersecurity infrastructure when the government of India's annual budget was unveiled in February 2023 (Figure 4.6).

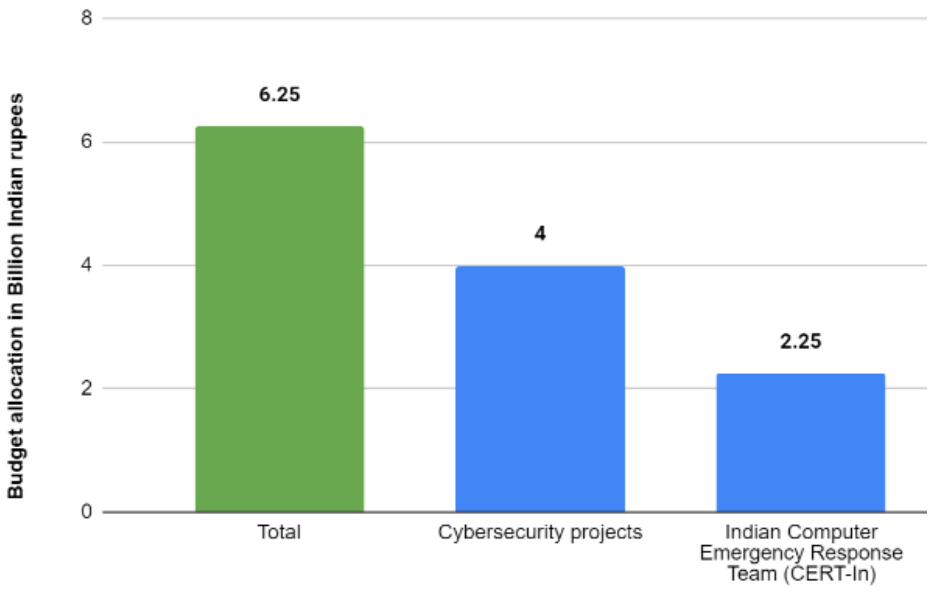

Figure 4.8: Government budget allocation for cybersecurity in India

The Indian Computer Emergency Response Team (CERT-In), the nation's preeminent authority on cybersecurity regulation, was allocated more than two billion rupees of this amount. (29)

Industry Leaders Strongly Support the Indian Government's Plan to Double Cybersecurity Funding from Rs 400 Cr to Rs 750 Cr in the 2024 Interim Budget. India's cybersecurity scene is about to take a big turn because of a decision the Indian government made that would be reflected in the interim budget for 2024. (60)

SECTION 5

Case Study: **AIIMS Ransomware Attack**

Incident: On November 23rd, 2022, the All-India Institute of Medical Sciences (AIIMS) Delhi fell victim to a ransomware attack. The attack corrupted their systems, forcing them to switch to manual operations for over two weeks.

Background: AIIMS, renowned for its cutting-edge medical research and patient care, houses a vast trove of sensitive medical records, including those of high-ranking officials and VIPs. The institution's prominence made it a prime target for cybercriminals seeking to exploit valuable data for financial gain.

Impact:

- Disruption of critical hospital services: Appointment booking, billing, and diagnostics reporting were all unavailable.
- Potential data breach: Sensitive data of 40 million patients (57), including VIPs and political leaders, was compromised.
- Loss of trust: The attack exposed vulnerabilities in AIIMS's cybersecurity measures.
- Financial losses: The cost of restoring systems and potential legal ramifications are unknown.

Cause:

- Improper network segmentation: The lack of proper network segmentation allowed the attackers to gain access to critical systems (62).
- Outdated systems: AIIMS servers lacked essential security updates, making them susceptible to attack.

- Weak cybersecurity culture: The absence of staff training, security audits, and official email usage practices contributed to the attack's success.
- Response:
- Emergency response: Teams from CERT-In and the National Informatics Centre (NIC) worked to restore systems and investigate the attack.
- Police investigation: The Delhi Police filed an FIR under the IT Act's cyber terrorism section.
- National response: The attack prompted the formulation of a National Cybersecurity Response Framework (NCRF) to address vulnerabilities in critical infrastructure.

Lessons Learned:

- Importance of network segmentation: Segmenting networks can limit the attacker's reach within the system.
- Regular updates: Maintaining updated systems with the latest security patches is crucial to prevent attacks.
- Strong cybersecurity culture: Investing in staff training, security audits, and secure communication practices is essential.
- Disaster recovery plan: Having a plan in place ensures a faster and more efficient response to cyberattacks.

Open Issues:

- Data breach confirmation: The extent of the data breach and whether any patient information was leaked remain unclear.
- Attackers' identity: The identity of the attackers and their motives are still under investigation.

- Effectiveness of NCRF: The effectiveness of the newly formulated National Cybersecurity Response Framework remains to be seen.

This case study highlights the critical need for robust cybersecurity measures in healthcare institutions. The AIIMS attack serves as a wake-up call for increased vigilance and proactive measures to protect sensitive patient data and ensure the continuity of essential medical services.

SECTION 6

DISCUSSION

The paper Vulnerabilities in the System: Unravelling the Root Causes of Cyberattacks on Indian Healthcare provides information on the several kinds of cyberattacks that take place in the nation as well as their underlying causes. It draws attention to the weaknesses in Indian healthcare. In order to improve cyber security in this crucial industry, this discussion section explores the issues in more detail and offers some possible solutions.

6.1 The increasing need for regulation of AI

It is anticipated that the Indian data security market would reach a valuation of USD 261 million by 2025, from its 2019 valuation of USD 99.55 million.(3)

It is a fact that by introducing machine learning algorithms, predictive modelling, and sophisticated analytics, artificial intelligence (AI) improves healthcare systems. Large-scale datasets can be analysed by these algorithms, which can reveal patterns in illness, treatment results, and individualized healthcare advice (63).

However, the application of AI also adds more levels of complexity to the problems with data security. Concerns regarding possible weaknesses in data security are raised by the frequent information sharing between systems that occurs as AI algorithms learn and adapt. A careful legal framework is required to handle problems like algorithmic biases, unlawful access, and data breaches (63).

The current state of AI has shown that, with certain precautions taken, it may undoubtedly assist in resolving cyber security concerns. However, further regulation of AI is still necessary. In a 2023 cybersecurity readiness poll, when asked about aspects that may support

the expansion and seamless operation of their enterprises, 46% of the CEOs and CISOs surveyed throughout India cited the need for regulation of AI. The harmonization of cyber and data protection regulations in their respective operational regions came next (15).

6.2 Global Best Practices in Cybersecurity

Growing consumption of technology and a lack of knowledge about cyber security could be two major contributing factors to the nation's rising rate of cybercrime (31).

The main procedures that adhere to the recommendations that are now implemented and adopted in order to provide security can be categorized as follows (21):

- Data masking;
- Data confidentiality by encryption;
- Database Standards Compliance and Monitoring (DSCM);
- Datasets Classification and Assessment of User Rights Management
- Monitoring and Compliance with Database Standards

Electronic health records, or EHRs, are databases that contain PHI in electronic form and necessitate the implementation of security protocols. Maintaining regular backups of the datasets, encrypting data and storing it using strong encryption techniques, using antivirus software, limiting access with strong passwords, implementing multi factor authentication, patching operating systems on a regular basis, and securing the channel with secure socket layer (SSL) to prevent security lapses for the dataset in motion or at rest are just a few of the compliant security standards adopted globally(21).

6.3 HIPAA Practices: A Model for Recommendations

Healthcare providers are required to comply with security laws, such as those mandated by the Health Insurance Portability and Accountability Act (HIPAA) in US countries (12). The major practices followed under HIPAA are shown in figure 6.3.

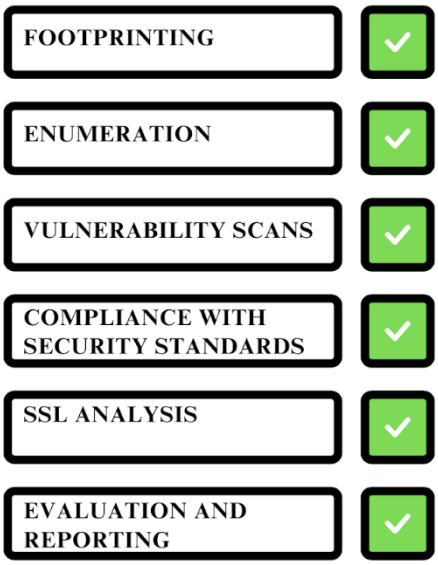

Figure 6.3: Major practices under HIPAA(12)

The best security measures include firewalls, email security gateways, intrusion detection and prevention systems (IDPS), privileged access management, data loss prevention systems (DLP), single sign-on (SSO), mobile device management (MDM), encryption, patch and vulnerability management, network monitoring tools, and zero trust solutions(12).

6.4 Countermeasures: Prevention Techniques for Cyber Attacks

Securing digital assets is the primary objective of cyber security. The following typical methods for preventing cyberattacks can lower the danger to a system, as indicated in table 6.4, monitoring and recording intrusion prevention systems and firewalls, malware detectors, password security and access control, encryption of disks, etc(4).

- **Infrastructure Modernization:** Healthcare institutions need to invest in modernizing their IT infrastructure with a focus on robust security features. This includes implementing firewalls, intrusion detection/prevention systems, and data encryption. (Source: NDHM Blueprint Standards and Regulations)
- **Network Segmentation Strategy:** Implementing a well-defined network segmentation strategy is crucial. This involves dividing the network into smaller sub-networks, each with its own security controls and limited access to other segments. This can significantly hinder an attack's ability to spread laterally. (Source: Cybersecurity best practices from National Institute of Standards and Technology (NIST))
- **Comprehensive Security Awareness Training:** Healthcare institutions must prioritize ongoing cybersecurity training programs for all staff members. These programs should educate them on cyber threats, social engineering tactics, data security best practices, and proper use of technology. (Source: NDHM Blueprint - Functional Principles - Educate and Empower)
- **Building a Strong Cybersecurity Culture:** Leadership support is crucial for fostering a culture of cyber awareness within the healthcare organization. This involves integrating security considerations into daily operations, conducting regular security audits and vulnerability assessments, and prioritizing timely security updates. (Source: Healthcare Sector Cybersecurity Framework from Health Sector Cybersecurity Coordination Working Group (HSCWG))
- **Strengthening the Legal Framework:** The swift enactment and effective implementation of the DISHA Act are critical steps towards a more robust legal framework for cyber security in healthcare. This act should clearly define data security responsibilities, outline incident reporting procedures, and establish

appropriate penalties for cybercrimes targeting healthcare institutions. (Source: Discussion on Proposed DISHA Act in the research report)

CYBER ATTACKS	KEY TERMS	CYBER SECURITY AREAS	BENEFITS	GOALS	PREVENTION TECHNIQUES
Denial of service	Make the system unavailable to authorized users.	Network Security	Protects networking components from threats.	Integrity, Availability	Firewalls, Auditing and Logging
Cross scripting	Attacker inserts malicious code and exploits the service user.	Web Security	Protects website from threats	Confidentiality, Integrity	Malware Scanners.
Hacking	Gaining access to information in an unauthorized manner.	Information Security	Protects digital and nondigital information from threats.	Integrity, Confidentiality	Firewalls, Access control and password security
Ransomware	Malware that locks the victim's computer.	Operational Security	Protects from various operations.	Integrity, Availability	Malware Scanners
Phishing	Sending fraudulent emails that appear to be from trusted sources.	Application Security	Protects applications from external threats	Integrity, Confidentiality	Firewalls, Access control and password security
Man-in the middle	Criminal enters a conversion between two parties and gains information.	Information Security	Protects digital and non-digital information from threats.	Integrity, Confidentiality	Intrusion Prevention Systems

Table 6.4: Cyber-attack prevention techniques (4)

Listed above are some suggestions on various cyberattacks, cybersecurity domains, objectives, and defence strategies. By using these strategies, one may ensure that their information systems are safe from cybercrimes. In the case of healthcare information systems, in particular, it should be required to take all necessary precautions to safeguard the most valuable data ever.

SECTION 7

CONCLUSION

The research reveals that network segmentation is very important for reducing the effects of cyber-attacks (figure 4.7). In most healthcare institutions, no proper network segmentation exists resulting in a scenario where hacking one part can easily result in hacking of the entire system. This "domino effect" thus gives attackers access to a wider range of sensitive data and critical systems. The case of the AIIMS attack in 2023 demonstrates how improper network segmentation enhances the consequences of a cyberattack.

Securing the network through proper segmentation

Network segmentations should be given priority by healthcare institutions, so as to isolate sensitive data and critical systems. By creating small sub-networks within the network each having its own security controls will attain this objective. The limited access and flow of information between these segments can greatly impede lateral movement of a cyberattack through the network. Nevertheless, while segmentation strategies must be customized to fit each institution's specific requirements, it is integral nevertheless to retain the principle of keeping sensitive data separate.

Strengthening government laws and policies

Government initiatives play an important role in enhancing cyber security in critical sectors such as health care. The National Cybersecurity Response Framework (NCRF) provides a standardized approach for incident response; however, successful deployment within healthcare institutions will determine its effectiveness.

The existing laws on cyber security in healthcare may need revision. While the Information Technology Act (IT Act) provides a base, it may not be adequate for dealing with emerging

cyber threats originating from the health care sector. DISHA (Digital Information Security in Healthcare Act) has outlined legislation that could offer an improved framework on data security and privacy within the health care system waiting for approval by the Parliament. It is necessary to pass and implement this act as fast as possible.

Building a strong cybersecurity culture in India

Developing a strong cybersecurity culture is one of the key steps towards a safer healthcare ecosystem. In order to achieve this, there must be ongoing training for healthcare practitioners on cyber threats, efficient data protection practices and technology use. The support from leaders should help in ranking cyber security first and integrating it into day-to-day operations thus enhancing compliance programs within the organization. By conducting regular phishing simulations and performing vulnerability assessments, these weaknesses can be identified.

Overall, the findings of this study states that cyber security for Indian healthcare is not a one-time solution but an ongoing process. A multi-faceted approach that involves increased awareness among healthcare institutions; modernizing infrastructure; securing applications; collaborating with stakeholders; and strengthening the legal framework is required here. By prioritizing cyber security, healthcare institutions can protect sensitive patient data, ensure the continuity of essential services, and build trust with patients in the digital age.

BIBLIOGRAPHY

1. Churi P, Pawar A, Moreno-Guerrero AJ. A Comprehensive Survey on Data Utility and Privacy: Taking Indian Healthcare System as a Potential Case Study. Inventions. 2021 Sep;[cited 2024 May 17]. Available from: https://www.mdpi.com/2411-5134/6/3/45

2. Aravamudhan P, T K. A novel adaptive network intrusion detection system for internet of things. PLoS One. 2023 Apr 21;[cited 2024 May 17]18(4):e0283725. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10121003/

3. Prasuna A, Rachh A. A study on challenges of data security and data privacy in the healthcare sector: Swot analysis. Asia Pacific Journal of Health Management. 2023 Mar;[cited 2024 May 4]18(1):283–9. Available from: https://search.informit.org/doi/abs/10.3316/informit.014727326511420

4. Nirmala AP, Asha V, Ramesh BN, Chandana K, Chandana GR, Alam A. A Systematic Review on classification of Cyber Attacks and its Prevention techniques to improve Cyber Security. In: 2023 International Conference on Computer Communication and Informatics (ICCCI) [Internet]. 2023 [cited 2024 May 4]. p. 1–6. Available from: https://ieeexplore.ieee.org/abstract/document/10128642

5. Alawida M, Omolara AE, Abiodun OI, Al-Rajab M. A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University - Computer and Information Sciences. 2022 Nov [cited 2024 May 4]1;34(10, Part A):8176–206. Available from: https://www.sciencedirect.com/science/article/pii/S1319157822002762

6. Vijarania M, Gupta S, Agrawal A, Misra S. Achieving Sustainable Development Goals in Cyber Security Using AIoT for Healthcare Application. In: Misra S, Siakas K, Lampropoulos G, editors. Artificial Intelligence of Things for Achieving Sustainable Development Goals [Internet]. Cham: Springer Nature Switzerland; 2024 [cited 2024 May 4]. p. 207–31. Available from: https://doi.org/10.1007/978-3-031-53433-1_11

7. Najar AA, Naik S M. Covid-19 Impact on Cyber Crimes in India: A Systematic Study. In: 2022 IEEE India Council International Subsections Conference (INDISCON) [Internet]. 2022 [cited 2024 May 4]. p. 1–8. Available from: https://ieeexplore.ieee.org/abstract/document/9862935

8. Sharma A, Gupta S. Cyber Crimes during COVID-19 Pandemic in India and World. Supremo Amicus. 2022; [cited 2024 May 4]; 29:[147]. Available from: https://heinonline.org/HOL/LandingPage?handle=hein.journals/supami29&div=16&id=&page=

9. Chithaluru P, Tanwar R, Kumar S. Cyber-Attacks and Their Impact on Real Life: What Are Real-Life Cyber-Attacks, How Do They Affect Real Life and What Should

We Do About Them? In: Information Security and Optimization. Chapman and Hall/CRC; 2021.

10. Chandani P, Rajagopal S, Bishnoi AK, Verma V. Cyber-Physical System and AI Strategies for Detecting Cyber Attacks in Healthcare. International Journal of Intelligent Systems and Applications in Engineering. 2023 Jul 11;11(8s):55–61.

11. Bhukya CR, Thakur P, Mudhivarthi BR, Singh G. Cybersecurity in Internet of Medical Vehicles: State-of-the-Art Analysis, Research Challenges and Future Perspectives. Sensors (Basel). 2023 Sep 27;23(19):8107.

12. Mohamad Al-Aboosi AM, Huda Sheikh Abdullah SN, Murah MZ, AL Dharhani GS. Cybersecurity Trends in Health Information Systems. In: 2022 International Conference on Cyber Resilience (ICCR) [Internet]. 2022 [cited 2024 May 4]. p. 01–4. Available from: https://ieeexplore.ieee.org/abstract/document/9995952

13. Chintala SK. DATA PRIVACY AND SECURITY CHALLENGES IN AI-DRIVEN HEALTHCARE SYSTEMS IN INDIA.

14. Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, et al. Healthcare Data Breaches: Insights and Implications. Healthcare (Basel). 2020 May 13[cited 2024 May 4];8(2):133. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/

15. Statista [Internet]. [cited 2024 May 4]. India: regulation impact on cybersecurity 2023. Available from: https://www.statista.com/statistics/1428306/india-impact-of-regulations-on-cybersecurity/

16. Malhotra P, Singh Y, Anand P, Bangotra DK, Singh PK, Hong WC. Internet of Things: Evolution, Concerns and Security Challenges. Sensors (Basel). 2021 Mar 5;21(5):1809.

17. Dubey A, Tiwari G, Dixit A, Mishra A, Pandey M. Leveraging Innovative Technologies for Ransomware Prevention in Healthcare: A Case Study of AIIMS and Beyond. In: Chaturvedi A, Hasan SU, Roy BK, Tsaban B, editors. Cryptology and Network Security with Machine Learning. Singapore: Springer Nature; 2024. p. 711–30.

18. Making India's healthcare sector cybersecurity - ProQuest [Internet]. [cited 2024 May 5]. Available from: https://www.proquest.com/docview/2874610517/citation/AF230932D6ED4177PQ/1?sourcetype=Trade%20Journals

19. Overcoming cybersecurity challenges in healthcare - ProQuest [Internet]. [cited 2024 May 5]. Available from: https://www.proquest.com/docview/2814599977/AF230932D6ED4177PQ/2?sourcetype=Trade%20Journals

20. Purvi Nema N, Riya Sinha N. Privacy And Security Concerns In Electronic Health Records - A Comparative Study Between India And USA. Journal of Law and Legal

Studies [Internet]. [cited 2024 May 4];1(1). Available from: https://hcommons.org/deposits/item/hc:43075/

21. Kakarla S, Rao DN, Kakarla G, Gorla S. Statistical Trend in Cyber Attacks and Security Measures. In: Computational Intelligent Security in Wireless Communications. CRC Press; 2023[cited 2024 May 17]. Available from: https://www.taylorfrancis.com/chapters/edit/10.1201/9781003323426-14/statistical-trend-cyber-attacks-security-measures-shirisha-kakarla-deekonda-narsinga-rao-geeta-kakarla-srilatha-gorla

22. Dhanare R, Sharma PC, Kumar Srivastava D. Vulnerabilities, Attacks and Solutions of Cybersecurity in Medical Domain. In: 2021 International Conference on Computational Performance Evaluation (ComPE) [Internet]. 2021 [cited 2024 May 4]. p. 034–9. Available from: https://ieeexplore.ieee.org/abstract/document/9751911(1)

23. Statista [Internet]. [cited 2024 May 5]. Cyber attacks in healthcare sector worldwide by type 2022. Available from: https://www.statista.com/statistics/1362863/cyber-attacks-on-healthcare-organizations-worldwide-by-type/
24. Statista [Internet]. [cited 2024 May 5]. Cybersecurity: market data & analysis. Available from: https://www.statista.com/study/124902/cybersecurity-report/

25. IBM Newsroom [Internet]. [cited 2024 May 5]. IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs. Available from: https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs

26. IBM India News Room [Internet]. 2019 [cited 2024 May 17]. IBM Report: Average cost of a data breach in India touched INR 179 million in 2023. Available from: https://in.newsroom.ibm.com/IBM-Report-Average-cost-of-a-data-breach-in-India-touched-INR-179-million-in-2023

27. Data Security Council of India (DSCI) [Internet]. 2023 [cited 2024 May 17]. DSCI: India Cyber Threat Report. Available from: https://www.dsci.in/files/content/knowledge-centre/2023/India-Cyber-Threat-Report-2023_0.pdf

28. Statista [Internet]. [cited 2024 May 5]. India: estimated cybersecurity market size 2028. Available from: https://www.statista.com/statistics/1197074/india-estimated-cybersecurity-market-size/

29. Statista [Internet]. [cited 2024 May 5]. India: government spending on cybersecurity 2023. Available from: https://www.statista.com/statistics/1428411/india-government-spending-on-cybersecurity/

30. Statista [Internet]. [cited 2024 May 17]. Global cyberattacks in industries 2023. Available from: https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/

31. Statista [Internet]. [cited 2024 May 5]. India: number of cyber crimes related to data theft 2022. Available from: https://www.statista.com/statistics/875925/india-number-of-cyber-crimes-related-to-data-theft/

32. Statista [Internet]. [cited 2024 May 5]. India: number of digital forgery incidents by leading state 2022. Available from: https://www.statista.com/statistics/1098541/india-number-of-digital-forgery-incidents-by-leading-state/

33. 5 cyber security trends that we may see in 2024. The Times of India [Internet]. 2024 Jan 24 [cited 2024 May 5]; Available from: https://timesofindia.indiatimes.com/gadgets-news/5-cyber-security-trends-for-2024-insights-and-predictions/articleshow/107093195.cms

34. Statista [Internet]. [cited 2024 May 5]. India: opinion on cybersecurity budgets in 2024. Available from: https://www.statista.com/statistics/1349789/india-opinion-on-cybersecurity-budgets/

35. Statista. [cited 2024 May 5]. Topic: Cyber crime in India. Available from: https://www.statista.com/topics/5054/cyber-crime-in-india/

36. Cybersecurity | Digital | McKinsey & Company [Internet]. [cited 2024 May 5]. Available from: https://www.mckinsey.com/capabilities/mckinsey-digital/mckinsey-technology/overview/cybersecurity

37. Cybersecurity is a requisite for unleashing 5G's potential in healthcare | McKinsey [Internet]. [cited 2024 May 5]. Available from: https://www.mckinsey.com/br/en/our-insights/all-insights/ciberseguranca-e-condicao-para-destravar-potencial-da-saude-com-5g

38. Cybersecurity trends: Looking over the horizon | McKinsey [Internet]. [cited 2024 May 5]. Available from: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon

39. 5 cyber security trends that we may see in 2024. The Times of India [Internet]. 2024 Jan 24 [cited 2024 May 5]; Available from: https://timesofindia.indiatimes.com/gadgets-news/5-cyber-security-trends-for-2024-insights-and-predictions/articleshow/107093195.cms

40. (6) Healthcare Sector is the Biggest Target for Cyber Attacks | LinkedIn [Internet]. [cited 2024 May 5]. Available from: https://www.linkedin.com/pulse/healthcare-sector-biggest-target-cyber-attacks-prof-r-s-nehra/

41. Biggest Healthcare Industry Cyber Attacks | Arctic Wolf [Internet]. [cited 2024 May 5]. Available from: https://arcticwolf.com/resources/blog/top-healthcare-industry-cyberattacks/

42. Cert-In - Home Page [Internet]. [cited 2024 May 5]. Available from: https://www.cert-in.org.in/s2cMainServlet?pageid=PUBANULREPRT

43. cyber attacks: State-sponsored cyberattacks against India up 278% in three years - The Economic Times [Internet]. [cited 2024 May 5]. Available from: https://economictimes.indiatimes.com/tech/technology/india-most-targeted-country-by-cyber-attackers-report/articleshow/104989856.cms

44. Lohchab H. Cyberattacks on healthcare sector rising, 60% of organisations hit in a year: report. The Economic Times [Internet]. 2023 Nov 3 [cited 2024 May 5]; Available from: https://economictimes.indiatimes.com/tech/technology/cyberattacks-on-healthcare-sector-rising-60-of-organisations-hit-in-a-year-report/articleshow/104917689.cms?from=mdr

45. Digital India Act: Here's how it should fix India's cybersecurity weaknesses [Internet]. [cited 2024 May 5]. Available from: https://www.moneycontrol.com/news/opinion/digital-india-act-heres-how-it-should-fix-indias-cybersecurity-weaknesses-11038701.html

46. Business Today [Internet]. 2023 [cited 2024 May 5]. India is the 10th most affected country by cyberattacks in 2022 with healthcare sector most impacted: Report. Available from: https://www.businesstoday.in/technology/news/story/india-is-the-10th-most-affected-country-by-cyberattacks-in-2022-with-healthcare-sector-most-impacted-report-399963-2023-09-27

47. mint [Internet]. 2024 [cited 2024 May 5]. India witnesses 15% rise in cyber attack cases in 2023. Available from: https://www.livemint.com/news/india/india-witnesses-15-rise-in-cyber-attack-cases-in-2023-emerges-as-2nd-most-targeted-nation-11705939863447.html

48. Ahaskar A. mint. 2022 [cited 2024 May 5]. Indian healthcare sector suffers 1.9 million cyberattacks in 2022. Available from: https://www.livemint.com/technology/tech-news/indian-healthcare-sector-suffers-1-9-million-cyberattacks-in-2022-11669878864152.html

49. Standard B. Indian websites faced over 5 billion cyberattacks in 2023, shows data [Internet]. 2024 [cited 2024 May 5]. Available from: https://www.business-standard.com/india-news/indian-websites-faced-over-5-billion-cyberattacks-in-2023-shows-data-124021501548_1.html

50. Ford N. IT Governance UK Blog. 2024 [cited 2024 May 5]. List of Data Breaches and Cyber Attacks in 2023 – 8,214,886,660 records breached. Available from: https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023

51. Page not found [Internet]. IHF. [cited 2024 May 5]. Available from: https://ihf-fih.org/artificial-intelligence-and-cybersecurity-in-healthcare/

52. Ransomware is highest cyber threat in India: Report – India TV [Internet]. [cited 2024 May 5]. Available from: https://www.indiatvnews.com/technology/news/ransomware-is-highest-cyber-threat-in-india-report-2024-03-21-922569

53. The Latest Cyber Crime Statistics (updated May 2024) | AAG IT Support [Internet]. [cited 2024 May 5]. Available from: https://aag-it.com/the-latest-cyber-crime-statistics/

54. The Wire: The Wire News India, Latest News,News from India, Politics, External Affairs, Science, Economics, Gender and Culture [Internet]. [cited 2024 May 5]. Available from: https://thewire.in/tech/nearly-60-of-healthcare-organisations-in-india-hit-by-cyberattacks-in-past-year-report

55. 5 Ways Indian Medical Administrations Can Boost Hospital Cyber-security - Forbes India [Internet]. [cited 2024 May 5]. Available from: https://www.forbesindia.com/article/iim-calcutta/5-ways-indian-medical-administrations-can-boost-hospital-cybersecurity/84397/1

56. Hindustan Times [Internet]. 2023 [cited 2024 May 5]. AIIMS ransomware attack led to new SOP on cyber breaches: Ex-cybersecurity chief Pant. Available from: https://www.hindustantimes.com/india-news/aiims-ransomware-attack-led-to-new-sop-on-cyber-breaches-ex-cybersecurity-chief-pant-101688321198625.html

57. AIIMS ransomware attack: what it means for health data privacy, ET CISO [Internet]. [cited 2024 May 5]. Available from: https://ciso.economictimes.indiatimes.com/news/aiims-ransomware-attack-what-it-means-for-health-data-privacy/96538957

58. Desk DW. Deccan Herald. [cited 2024 May 5]. Data of 81.5 crore citizens up for sale in “biggest” data breach in India: Report. Available from: https://www.deccanherald.com/india/data-of-815-crore-citizens-up-for-sale-in-biggest-data-breach-in-india-report-2749794

59. Statista [Internet]. [cited 2024 May 5]. India: number of cyber crimes related to data theft 2022. Available from: https://www.statista.com/statistics/875925/india-number-of-cyber-crimes-related-to-data-theft/

60. Indian Government Doubles Cybersecurity Funding from Rs 400 Cr to Rs 750 Cr in 2024 Interim Budget: Industry Leaders Strongly Advocate [Internet]. [cited 2024 May 17]. Available from: https://cxotoday.com/specials/indian-government-doubles-cybersecurity-funding-from-rs-400-cr-to-rs-750-cr-in-2024-interim-budget-industry-leaders-strongly-advocate/

61. Network Segmentation and How it Can Prevent Ransomware [Internet]. 2024 [cited 2024 May 17]. Available from: https://www.threatintelligence.com/blog/network-segmentation

62. www.ETHealthworld.com. ETHealthworld.com. [cited 2024 May 17]. From AIIMS Delhi to ICMR, data breaches haunt crores of Indians - ET HealthWorld. Available from: https://health.economictimes.indiatimes.com/news/health-it/from-aiims-delhi-to-icmr-data-breaches-haunt-crores-of-indians/105173060

63. Chintala SK. DATA PRIVACY AND SECURITY CHALLENGES IN AI-DRIVEN HEALTHCARE SYSTEMS IN INDIA. [cited 2024 May 17] Available from: https://sjcjycl.cn/article/view-2022/2769.pdf

64. O'Brien Niki, Ghafur Saira, Sivaramakrishnan Arvind, Durkin Mike. Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that [Internet]. PubMed Central (PMC). 2022 [cited 13 April 2024]. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9210086/

65. Express Healthcare, Mumbai. Making India's healthcare sector cybersecurity resilient [Internet]. ProQuest (PQ). 2023 [cited 13 April 2024]. Available from: https://www.proquest.com/docview/2874610517/fulltext/AF230932D6ED4177PQ/1?accountid=136944&sourcetype=Trade%20Journals

66. Ayushman Bharat. National Digital Health Blueprint [Internet]. [cited 6 July 2024]. Available from: https://abdm.gov.in:8081/uploads/ndhb_1_56ec695bc8.pdf