CONHECIMENTO & DIVERSIDADE
ISSN 2237-8049
UnilaSalle Editora

AN EVIDENCE-BASED INVESTIGATION OF CERT-IN'S REPORTING ON CYBER-THREATS IN HEALTHCARE SECTOR

UMA INVESTIGAÇÃO BASEADA EM PROVAS DOS RELATÓRIOS DO CERT-IN SOBRE CIBERAMEAÇAS NO SECTOR DA SAÚDE

Niharika Raizada*
Gujarat National Law University, Gandhinagar
niharikaphd202030@gnlu.ac.in

Mamata Biswal
Gujarat National Law University, Gandhinagar
mbiswal@gnlu.ac.in

ABSTRACT

The pandemic underscored the significance of a digital health system. Healthcare sector has become one of the most important infrastructures since then. Undoubtedly, the digital health is the ultimate way to ensure accessibility, inclusiveness and delivery of healthcare services in an affordable and efficient manner. However, rising cyber-threat is one of the biggest concerns for healthcare organizations. The data breach incidents on Indian Council of Medical Research and on Covid-19 vaccine database in 2023 highlight the utter need to address the issue. To mitigate such incidents, India has established Computer Emergency and Response Team (CERT-In) which has been endowed with primary responsibility to prevent, treat, respond and report such threats. Although, CERT-In is responsible to report any cyber-incident but there is no information concerning the affected organizations and on frequency and severity of such cyber-incidents. It is doubtful as to how any authority is supposed to respond in lack of data or policy makers formulate a comprehensive framework to deal with the issue. CERT-In faces challenges in accurately reporting cyber incidents and contain discrepancies compared to other organizations' data and lacking detailed incident information. This research aims to analyze government records and secondary sources to understand the cyber-threat landscape, particularly in the healthcare industry. Using normative and comparative methods, it suggests measures which can be adopted by CERT-In based on assessments of U.S. and E.U. reporting practices. Findings stress the need for improved reporting practices and transparency in cybersecurity assessments to enhance data accuracy and completeness, urging policymakers and stakeholders to take action against cyber threats.

Keywords: Cyber-attacks, Healthcare, threat landscape, Governance, Incident Reporting, Administration, CERT-In.

RESUMO

A pandemia veio sublinhar a importância de um sistema de saúde digital. Desde então, o sector dos cuidados de saúde tornou-se uma das infra-estruturas mais importantes. Sem dúvida, a saúde digital é a melhor forma de garantir a acessibilidade, a inclusão e a prestação de serviços de saúde de uma forma acessível e eficiente. No entanto, a crescente ameaça cibernética é uma das maiores preocupações das organizações de saúde. Os incidentes de violação de dados no Conselho Indiano de Investigação Médica e na base de dados de vacinas contra a Covid-19 em 2023 realçam a necessidade absoluta de abordar a questão. Para atenuar esses incidentes, a Índia criou a Equipa de Emergência e Resposta Informática (CERT-In), que tem a responsabilidade principal de prevenir, tratar, responder e comunicar essas ameaças. Embora a CERT-In seja responsável pela comunicação de qualquer ciberincidente, não existem informações sobre as organizações afectadas, nem sobre a frequência e a gravidade desses ciberincidentes. É duvidoso como é que qualquer autoridade deve responder na falta de dados ou como é que os decisores políticos devem formular um quadro abrangente para lidar com a questão. O CERT-In enfrenta desafios na comunicação exacta de incidentes cibernéticos e contém discrepâncias em comparação com os dados de outras organizações e falta de informações detalhadas sobre os incidentes. Esta investigação visa analisar registos governamentais e fontes secundárias para compreender o panorama das ciberameaças, em especial no sector da saúde. Utilizando métodos normativos e comparativos, sugere medidas que podem ser adoptadas pelo CERT-In com base em avaliações das práticas de comunicação dos EUA e da UE. Os resultados sublinham a necessidade de melhorar as práticas de comunicação e a transparência nas avaliações de cibersegurança para aumentar a exatidão e a exaustividade dos dados, instando os decisores políticos e as partes interessadas a tomarem medidas contra as ciberameaças.

Palavras-chave: Ciberataques, cuidados de saúde, cenário de ameaças, governação, comunicação de incidentes, administração, CERT-In.

1. Introduction

The cyber-threat in India have wide landscape. In recent years, India has witnessed a rapid and transformative integration of digital technologies into various aspects from communication and commerce to governance and healthcare. While this digital revolution has brought about unprecedented convenience and efficiency, it has also given rise to a complex and evolving cyber-threat landscape. The paradigm shift towards a digital economy has made India not only a global player in the technology sector but also a prominent target for cyber adversaries.

Safeguarding health information systems has hence become crucial than ever for the organizations. Furthermore, the use of Internet of Things devices has substantially increased the attack surface for cybercriminals. Last few years have been very difficult for critical infrastructures. Disruptive attacks like Wannacry and NotPetya underscores the utter requirement of a robust cyber-infrastructure for the mitigating such risks. In addition to this the probability of these kind of attacks only

saw upsurge and adversely affected the whole functioning of the organization, directly affecting the consumers at a very critical point of time (Biasin, E. (2020).

Critical infrastructures like healthcare and financial industry has become a prime target for data theft, identity theft, ransomware attacks, etc. (Tully, J., Selzer, J., Phillips, J. P., O'Connor, P., & Dameff, C. (2020). The critical infrastructures have undergone a drastic age over the decade and subsequently viewed as a honeypot by the cybercriminals. As a result of this revolutionary digitization, the likelihood of data breach have also increased significantly. One crucial aspect which makes these sectors particularly susceptible to cyber-attacks and cybercriminals is utilization of supply chain, since these organizations require inter-connected network of other entities as well like different suppliers and other external services and function as an interoperable network of large amount of data (Abraham, C., Chatterjee, D., & Sims, R. R. (2019).

1.1 Cyber-threats and healthcare

The steep rise in cyber-threats in health sector is worrisome. Given the amount of sensitive information healthcare organizations store emphasize the need for a better recording, storing and exchange of information mechanism for information. Before the adoption of a comprehensive and integrated digital health system in India, there have been several incidents of cyber-incidents affecting the healthcare industry as whole. The primary motivation for initiating a cyber-attack on a healthcare organization is usually financial gain (Keshta, I., & Odeh, A. (2021). The cyber-criminals tend to sell the sensitive information like medical history, financial information, demographic details, etc. retrieved from a personal health record of an individual on black market. Such medical record is usually cost for approximately 1000$ (Ibarra, J., Jahankhani, H., & Kendzierskyj, S. (2019). Not only the individual face violation of their privacy but also faces the threat of his/her information being misused. The significance of an adequate cyber-infrastructure was highlighted when WannaCry Distributed Denial of Service Attack adversely affected the critical care services of NHS, UK in 2017. Similar incidents have occurred and affected critical infrastructure like healthcare institutions all over the

world. In India, a recent ransomware attack on All India Institute of Medical Sciences, Delhi led to encryption and loss of 1.3 Terabytes of personal data of patients, cessation of critical care services and financial loss to the healthcare infrastructure (Kumar, D, 2023). Besides this, Indian Council of Medical Research and CoWIN database also suffered data breach and loss of sensitive information of patients. In 2022, healthcare industry suffered 2.78 lakhs of cyber-attacks, next to US (Ghosh, S. (2022). The frequency of cyber-attacks will only be increasing with developing trends in technology hence it is of utmost necessity to mitigate such threats and respond timely in case of occurrence of a cyber-incident.

Furthermore, ensuring cybersecurity for protecting health information is not just a huge challenge for healthcare organizations in the dynamic realm of technology but is also an important concern for a nation. Inadequate robust cyber-infrastructure, governing policy, appropriate reporting method and response highlights the minimal concern of a nation towards cybersecurity. United States and European Union have formulated and implemented proper policies, reporting mechanisms and legal framework to mitigate such threats and respond timely in case of such incidents.

In India, Computer Emergency and Response Team (CERT-In) has been established as the first line of defense to respond in case of occurrence of any form of cyber-threat. The establishment of CERT-IN under central government in 2004 was one of the turning points that boosted country's cybersecurity. It is established by Central Government section 70B of the Information Technology act (IT Act), 2000 and operates as a central nodal agency that addresses the growing issues of cyber security. CERT – In is the leading actor in India's national cyber-defense, performing numerous functions, which include the gathering, processing, and sharing of essential data regarding the cybersecurity events within the country. The agency plays one of the most important roles that are necessary for reporting cyber events, giving general advice, providing forecasts, and issuing alerts concerning possible cybersecurity incidents. CERT-In publishes an annual report every year delineating the details of every reported cyber-incidents in the country, but there seems a huge inconsistency between records published by the nodal agency and non-

governmental organizations. The research aims to identify gaps in cyber-threat landscape affecting the healthcare industry and evaluates the efficiency of CERT-In for reporting cyber-threats. This exploration into the cyber-threat landscape in India aims to delve into the nuanced dimensions of cyber challenges and shedding light on the nature of threats. By examining the historical context, recent incidents, and emerging trends, we can gain insights into how CERT-In is navigating the intricate web of cyber threats, as well as the strategies being employed to safeguard its digital future.

2. Material and methods

2.1 Analytical Framework

The overall analytical approach employed a structured framework on quantitative and methodology. Quantitative analysis focused on the frequency of the cyber-threats. Comparative assessments and trend analyses were conducted to identify evolving patterns over the studied period. The analytical framework involves reviewing three different reports to achieve three objectives:

a. To determine the cyber-threat landscape in India.

b. To explore the trends of the attacking landscape in India.

c. To conglomerate the data extracted from three reports and form an integrated view of the overall landscape.

The integrated view aims to provide a holistic view of the cyber-threat landscape providing an in-depth view of the threats and the frequency of such threats.

The second part of the analysis involves comparing three different reports to achieve the objective to determine the cyber-threat landscape specifically for healthcare industry in India. This part involves selecting the reports which have primarily dealt with the cyber-threats affecting industry-wise in the year 2022. The analysis has been done on the basis of data extracted from two reports published by DSCI (India Cyber Threat Report. (2023), Seqrite (Seqrite annual threat report (2022) and CloudSek for the year 2022.

The research also analyzes policies and manner of reporting cyber-incidents by United States and European Union and suggests better reporting methods to enhance transparency in records published by CERT-In.

2.2 Hypotheses

CERT-In plays a significant role in cyber-threat intelligence however there significant concerns around adequacy and veracity of information disseminated in its reports. Upon overview of the records published by the institution for the year 2022, approximately 14 lakhs incidents were reported by affected organizations. Furthermore, lack of categorization of the different sectors affected highlight the absence of granularity and crucial details of these incidents. The deficiency in the records affect the decision-making of policy makers and other stakeholders and resultantly impact the privacy of individuals. On the basis of initial analysis, following hypotheses have been framed:

1. H_{1}- CERT-In reports does not possess detailed information on cyber-threats, resulting in substantial data gaps.
2. H_{2}: - CERT-In reports possess detailed information on cyber-threats, resulting in substantial data gaps.

Upon overview of CERT-In incident reporting mechanism disclose certain insufficiencies in recording and furnishing information related to cyber-threats. Regardless of the significant role of CERT-In, the organization's functioning with reference to reporting cyber-threats is inefficient and results in inaccurate information. In absence of reliable data, organizations as stakeholders face several challenges in identification of trends, allocation of resources and specific countermeasures and consequently leaving systems and networks vulnerable. The hypotheses under evaluation is, if the implementation of proper implementation of incident reporting procedure increases data collection system by CERT-In will refine reporting cyber-threats. Accordingly, the following hypotheses have been framed:

1. H_{3}-The incident reporting of CERT-In does not appropriately record and furnish information on cyber-threats, highlighting the inefficient processes.

2. H_4- The incident reporting of CERT-In appropriately records and furnishes information on cyber-threats.

2.3 Quantitative analysis of frequency of cyber-threats in India

This particular section highlights the methodology implemented for the purpose of analysis of cyber-threat landscape in India with a primary focus on the period of 2018-2023. The secondary source is the data obtained from Computer Emergency Response Team – India (CERT-In). However, it is relevant to note that there are certain challenges in the government records. The government records lack data categorization and lower updates in government records, complementary information was obtained from private organizations, especially Quick Heal and Seqrite was utilized to improve the depth and specificity of the analysis.

2.3.1 Collection of Data

The primary source for collection of data has been based on CERT-In. CERT-In is the National Nodal Agency established in 2003. CERT-In's primary objective involves analyzing cyber-incidents, issuing emergency measures to mitigate and coordinate response for cyber-incidents. Furthermore, CERT-In is also responsible to manage any cybersecurity related incident and provides support to adversely affected organizations. The extent of CERT-In's support differs and is subject to other factors like severity of incident, the size of affected enterprise and the possession of resources at the time of incident.

CERT-In, unlike other organizations which require harm-based approach which determines notifying supervising authority on the basis of severity of incident, Information Technology Act, 2000 obligates organizations to mandatorily notify CERT-In on occurrence of cyber-incidents (Misra, A., & Chacko, M. (2021). List of these incidents include, Targeted scanning or probing of critical networks or systems; compromise of critical systems or information; unauthorized access of information technology systems or data; defacement of websites; intrusions into websites; unauthorized changes to websites; malicious code attacks; attacks on servers; identity thefts; spoofing; phishing attacks; denial of service and distributed

denial of service attacks; attacks on critical infrastructure; supervisory control and data acquisition (SCADA) systems, and wireless networks;

2.3.2 Categorization of data

The CERT-In reports from 2018-2022 provide for five categories-

1. Phishing
2. Unauthorized probing or scanning of networks
3. Vulnerable services
4. Virus/ Malicious code
5. Others

2.3.3 Supplementary records from Quick Heal and Seqrite

2.3.3.1 Motivation for Inclusion

To address the issue of lack of categorization, data from reports by private organization specifically Quick Heal (*Quick Heal Annual Threat Report 2022*. (2023a) and Seqrite is utilized. These organizations is known for its wide-ranging analysis of different cybersecurity trends, incident response time and capability. The reports aims to supplement government data and also provide distinct insights into detailed threat kinds and their respective trends.

2.3.3.2 Data Extraction from Reports of Quick Heal and Seqrite

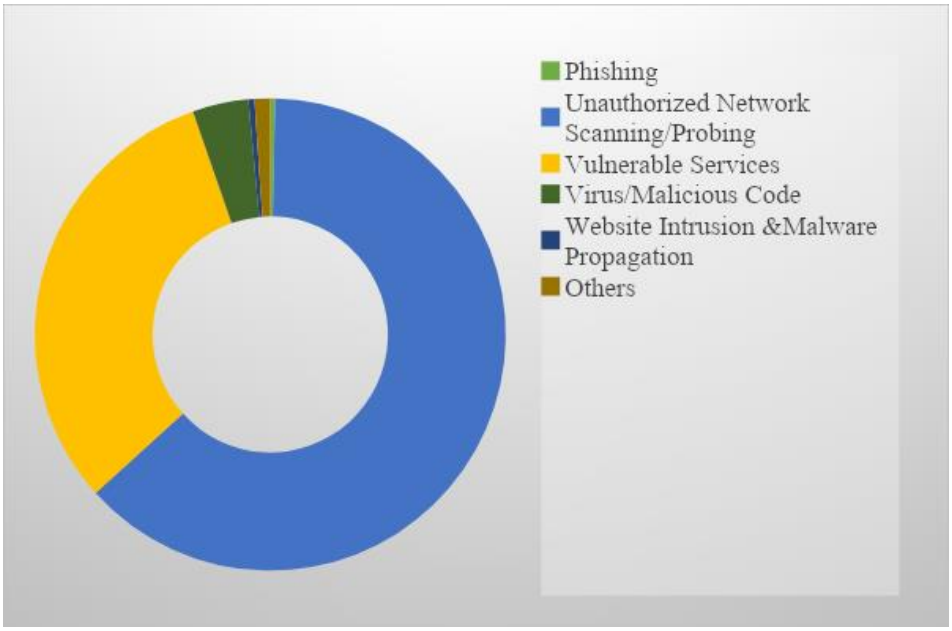
Relevant data from Quick Heal and Seqrite was systematically extracted and correlated it with CERT-In's data. This process enabled better categorization of threats like malware, ransomware, Distributed Denial of Services Attacks. The incidences of other cyber-threats are not limited to the incidents listed in CERT-In report from 2018-22. In addition to this, the reports offer different perspectives leading to same conclusions.

2.3.4 Data from CERT-In

2.3.4.1 Determining the threat landscape

CERT-In recorded for over 13 lakhs malign cyber-incidents occurred over the country. The CERT-In records show limited landscape of threats over one year. Furthermore, from the period of 2018-2022, the threat landscape comprises of phishing, unauthorized network scanning and probing, vulnerable services, malicious code, Others. It is important to note that the number of cyber-incidents recorded by CERT-In are 13, 85, 940 of which phishing is the most documented one. The overview of the 2022 threat landscape has been provided below in the pie-chart.

Figure 1 – Based on CERT-In Records (2023 Report) - [Pie-chart-1]

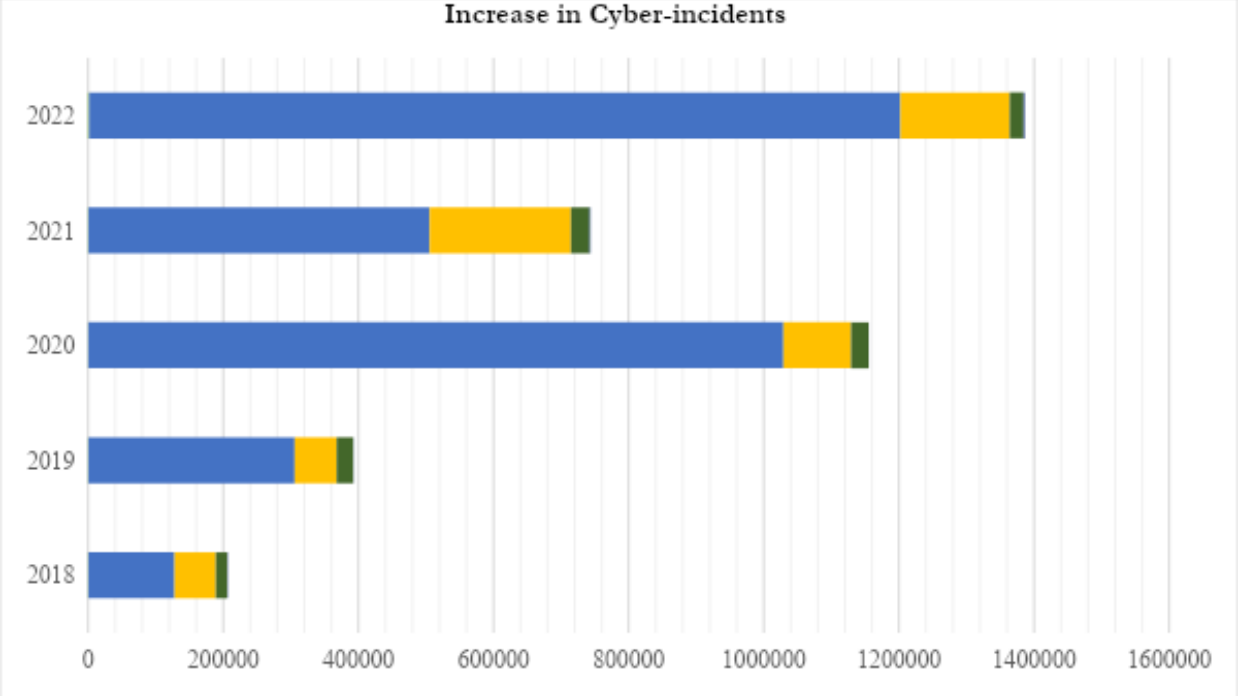


2.3.4.2 Cyber threat surge: a 5-year overview (2018-2022)

A steep rise has been observed in the number of different cyber-incidents in the pie chart. The line graph below provides for extensive overview of the above listed cyber-incidents have been provided in Figure- 2. The analysis has been solely based on the CERT-In report 2023. The trend demonstrated in the five year span shows the categories of cyber-threats and increase or decrease in their frequency.

The number of cyber-threats followed by the frequency of their occurrence were observed and recorded as depicted in the Figure-2.

Figure 2 – Increase in cyber-threats based on CERT-In Reported Cases (Bar graph-1)



2.3.5 Need for Integration of Data from Group- 1 Reports:

It is pertinent to note that records from CERT-In do not provide for comprehensive overview of the kinds of other cyber-threats include ransomware, malware, zero-day vulnerabilities, worm infections, distributed denial of services attacks and infectors. The integrated dataset from Group-1 Reports facilitated a comprehensive analysis of the cyber threat landscape in India. Commonalities and disparities between the datasets were explored to ensure the reliability and accuracy of the findings. The integrated data provided a more holistic view, incorporating both government and private sector perspectives on cyber threats.

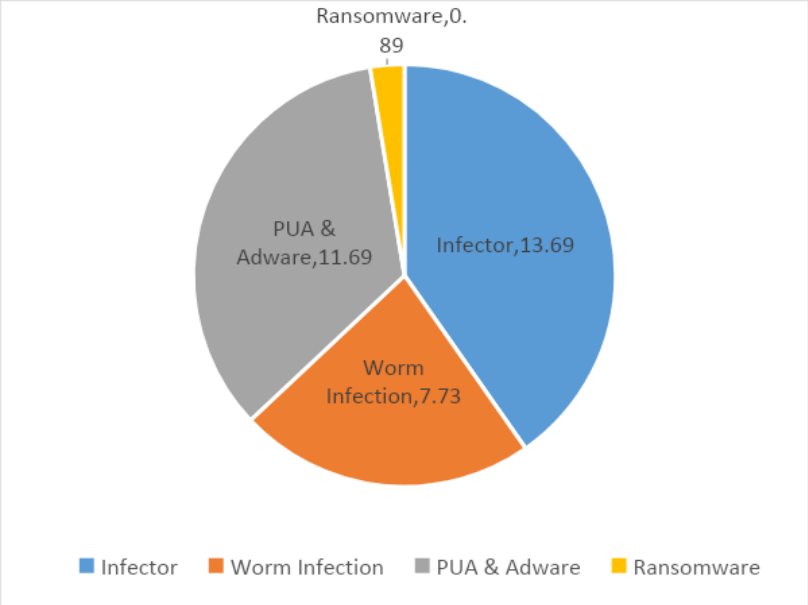
2.3.6 Seqrite Annual Threat Report 2023

Seqrite Annual Threat Report published in 2023 provides for a comprehensive overview of the different cyber-threats occurred in 2022. The report highlights the every kind of cyber-threats occurs every hour. The report also highlights the number of cyber-threats that happened over four quarters of the year. The report furthermore laid down key insights include quarterly malware detection, monthly malware detection along with category-wise and year on year and quarter on quarter malware statistics in May 2022. In addition to this, report also delves into ransomware trends and industry-wise trends and the most frequently affecting malware in different industries throughout 2022, potentially unwanted applications, adware, cryptojacking, network-based exploits. Lastly, the report highlights the five most affected cities and states.

The data extracted from Seqrite Report 2023 only includes the frequency of the incidents and not the severity. Furthermore, the industry-wise data has been excluded on account of reason that the data extracted from CERT-In records and Quick Heal reports do not categorize the threat landscape industry-wise and cross-checking of the data would not be possible. The focus is primarily on the quantitative analysis of the threats and does not delve into the qualitative aspect of the threats.

The threat-landscape in **Pie-chart-2** provides for the major cyber-threats highlighted in the report. The number of the cyber-threats are represented in millions (mn) occurred in 2022.

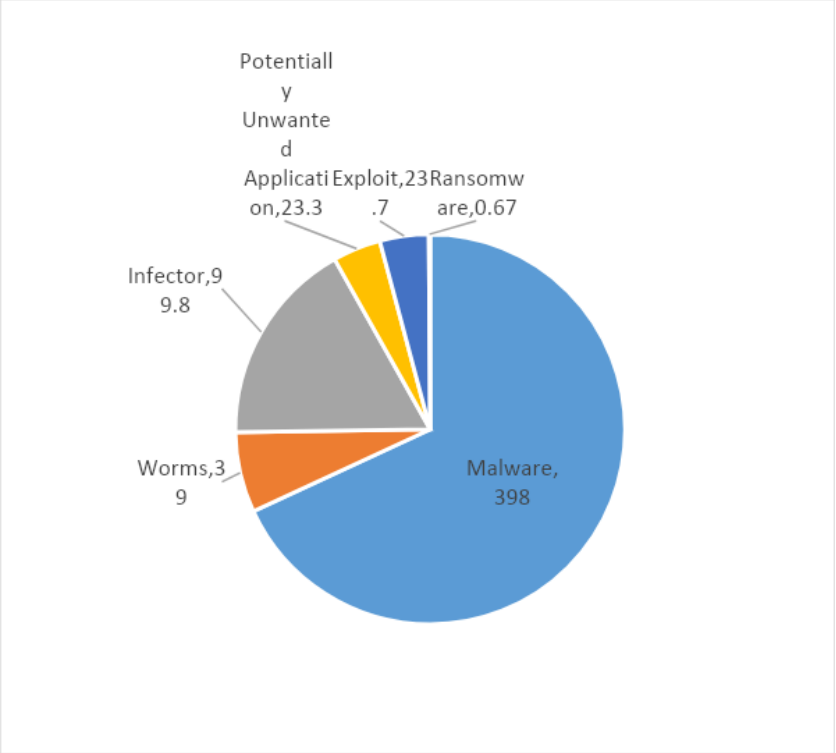
Figure 3 – Threat Landscape in India according to Seqrite Report (2023) [Pie chart-2]



2.3.7 Quick Heal Annual Threat Report 2023

Quick Heal Report for year 2023 (Quick Heal, 2023)—provides a comprehensive view of different types of window and android targeting cyber-threats over the year 2022. The report also showcases for quarterly trends for malware detection and comparison, ransomware detection and comparison, phishing statistics over the year. Besides this, the report also highlights the top five malware, potentially unwanted applications and adware and top five cities and the states which are adversely affected by different kinds of cyber-threats. The data extracted from the report includes windows affecting cyber-threats during the year of 2023 and only the frequency is taken into account and not their severity. The threat landscape in **Pie-chart- 3** provides for comprehensive view of different kinds of cyber-threats. These threats are represented in millions (mn) during 2022.

Figure 4 – Categorization on the basis of Quick Heal Report 2023 [Pie chart-3]



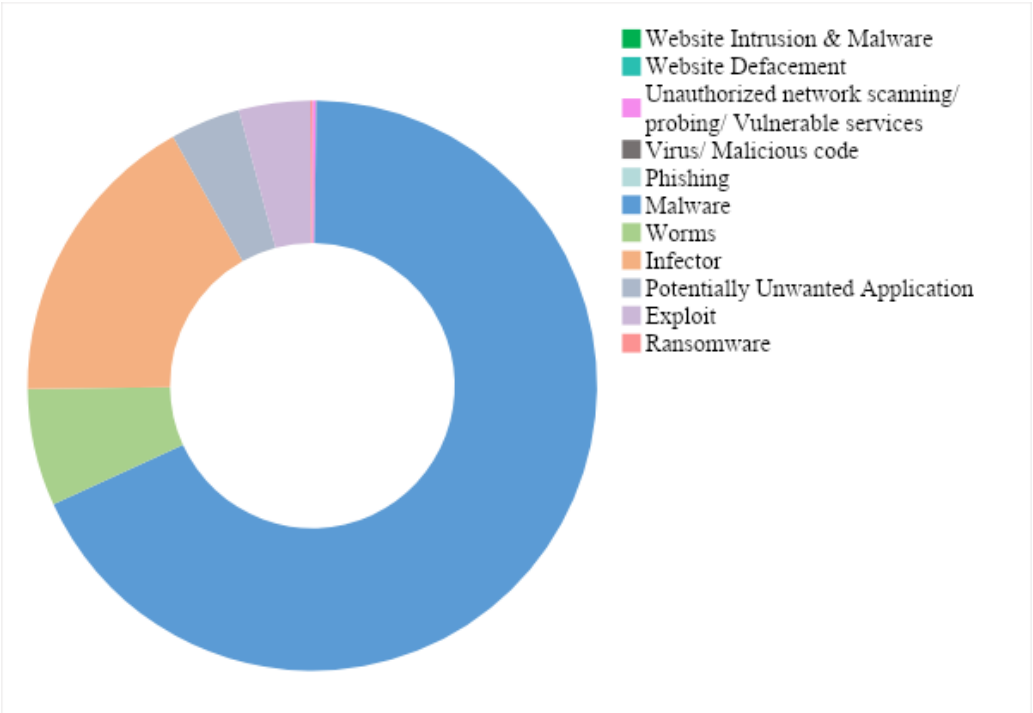
2.3.8 Preparation of Integrated Threat Landscape

Preparation of a unified structure of the cyber-risk matrix provides for holistic view of cyber-threats and the recent trends in 2022. The integrated version of Group-1 reports provided for following cyber-threats in 2022 and their frequency during the year. It is pertinent to note that the data extracted from reports published by Seqrite and Quick Heal have slight difference in certain types of cyber-threats. In addition to this, CERT-In records discusses only limited categories of the threats providing for an inadequate representation. A graphical representation of the data acquired from the three reports:

a. CERT-In records have been presented in Pie-chart -1,
b. Data acquired from Seqrite have been represented in Pie-chart-2 and,
c. Lastly, data obtained from Quick Heal Report has been represented in Pie-chart -3.

An integrated view of the cyber-threats has been represented in Pie- Chart -4 which widely covers most adversely affecting cyber-threats. The cyber-threats represented herein are of general nature and are not categorized industry-wise. For the sake of convenience, the three reports herein are considered here as Group- 1 reports.

Figure 5 – Integrated Categorization of Cyber-Threats based on Group -1 Reports [Pie chart-4]



3. Cyber-threats in healthcare industry

The lack of industry-wise categorization does not signify that healthcare industry has not suffered the adverse impact of the cyber-threats. There have been several cases where different healthcare organizations and institutions have been affected due to data breach incidents and threats. For the sole purpose of establishing a conception highlighting the significance of formulating a cyber-infrastructure for medical and healthcare industry, a brief review of four reports have been done. The reports in combination are designated as Group- 2 Reports for the sake of brevity and convenience.

3.1 Significance and Sampling:

The primary element for selecting the reports is determination of the presence of statistics related to cyber-threats landscape with respect to Indian healthcare industry. The rationale underscoring the analysis on the basis of above parameter is determination of the fact that healthcare industry is severely affected by the different kinds of cyber-threats. On the basis of the above criteria, the reports have been selected from Seqrite (*Seqrite annual threat report 2022*. (2022b), DSCI (*India Cyber Threat Report*. (2023b), CloudSek and IBM. The reports from Seqrite, Quick Heal and CloudSek (Mittal, A., Saxena , H., & Tripathi , I. (2022b) provide for the industry-wise categorization of the cyber-threats.

The significance of laying down such representation is emphasized with the statistics providing for the cost per data breach highlighted in report published by IBM (*Cost of Data Breach*. (2023) in 2023. The combined analysis of the four reports provide for rather a comprehensive view for different stakeholders and enable them to establish such measures to minimize the probability of such threats.

3.2 Increased Cyber Attacks on the Global Healthcare Sector - CloudSek Report:

CloudSek report published in 2022 provides for a comprehensive view of cyber-attacks on global healthcare industry. The report initially provides for a comparative statistics of cyber-attacks on healthcare industry in 2021 and 2022. In the subsequent part, it delineates the trends of cyber-attacks affecting healthcare industry in different areas which includes, North America, Asia-Pacific, Europe and South Africa. The most number of cyber-attacks were recorded in North America in two year span (2021-2022). However, Asia-Pacific (APAC) region stood second in the same category. In the APAC region, India has the most recorded cases of cyber-attacks amounting to approximately 26.3% of the cyber-attacks and at global level 7.1% which is similar to the number of cyber-attacks suffered by China and Italy. In addition to this, the report enunciates that the most common types of attacks affecting the healthcare industry were ransomware, phishing attacks, Distributed

Denial of Service Attacks, ransomware attacks, vulnerability attacks, exploits and cryptojacking.

3.3 Seqrite Annual Threat Report 2023

Seqrite Annual Threat Report 2023 provided categorization of cyber-threats in each industry during the year 2022. The reports specifies fourteen major industries in the country and the frequency of the cyber-threats for each industry throughout the year. According to the report, the healthcare industry is the sixth most adversely affected area with 2.74 million cyber-threats in one year preceded by IT/ITES, Government institutions, Education institutions, Manufacturing and Professional Services as the topmost industry being the most affected area with 14.38 million cyber-threats. The report even though does not provide for classification of different threats affecting each industry, but the fact that 2.74 million cyber-threat affect healthcare industry is evidence that industry is adversely influenced by the cyber-threats.

3.4 India Cyber-Threat Report by Data Security Council of India

The report published by DSCI provides for detailed version of the above reports. The report highlights the industry trends in the year 2023. The report highlighted that 60 percent of the healthcare organizations are affected by different kinds of cyber-threats. The report specifies 15 industries adversely affected by the cyber-threats. The top three industries affected are Automative supply chain, Government and Education with 13 percent, 10 percent and 10 percent respectively. The healthcare industry suffers 8 percent of the total cyber threats. The report further provides for detail of malware and ransomware detections every second followed by the number of detections every month separately for each month from December 2022 to November 2023.

3.5 Cost of Data Breach by IBM

The report is an evaluative document determining the total cost suffered by different countries as a consequence of every data breach incident. The report covers 553 breaches in 16 countries and 17 regions. India is one of these countries considered as a sample. The study has further highlighted that India has suffered of loss of USD 2.18 million in the year 2023 alone and 2.23 million USD in 2022. This statistics encompasses all kinds of data breach suffered by every institution of all kinds of industry.

4. Analysis

In the dynamic landscape of India's digital frontier, the persistent evolution of technology has ushered in unprecedented opportunities and conveniences, accompanied by an escalating threat landscape. As we stand at the intersection of technological advancement and the vulnerabilities inherent in cyberspace, a visual exploration of the cyber threat landscape becomes imperative. Two key visual representations, a pie chart categorizing types of cyber threats and a bar graph illustrating the increase in cyber threats from 2019 to 2023, along with a combined pie chart post-analysis of CERT-In, Quick Heal and Seqrite report offer an insightful lens into the complex challenges faced by India's cybersecurity ecosystem.

1. The **Pie chart-1** provides for representation of data extracted from CERT-In reports from period of 2018 to 2022. The **Pie chart-2** provides for representation of data retrieved from Seqrite Report and finally **Pie chart-3** provides for data obtained from Quick Heal Report.

2. The **Pie chart 4** serves as a comprehensive breakdown of the diverse array of cyber threats plaguing the nation, categorizing them into distinct segments. From the insidious infiltration of malware to the deceptive tactics of phishing, and the disruptive power of ransomware and potentially unwanted applications, this visual depiction highlights the multifaceted nature of cyber threats. It acts as a roadmap, guiding stakeholders towards a deeper understanding of the prevalent

risks and the need for targeted cybersecurity strategies tailored to combat each threat category effectively.

- The largest segment in the pie chart signifies the most prevalent type of cyber threat, and subsequent segments illustrate the relative proportions of other threat categories. This breakdown aids in prioritizing cybersecurity efforts, allowing stakeholders to focus on mitigating the most significant risks. Common cyber threats include, phishing, unauthorized network scanning and probing, virus/ malicious code and vulnerable services.

3. The **Pie chart- 4** categorizes cyber threats into distinct segments, offering a nuanced perspective on the multifaceted challenges faced by India in the digital realm.

- Malware, represented by the largest segment, underscores the persistent threat posed by malicious software designed to infiltrate systems, compromise data integrity, and disrupt normal operations. The prominence of malware highlights the need for robust antivirus solutions, regular system updates, and user education to thwart these insidious attacks.

- Phishing, illustrated as another significant segment, signifies the prevalence of deceptive tactics employed by cybercriminals to manipulate individuals into divulging sensitive information. This could include fraudulent emails, fake websites, or social engineering techniques.

- Ransomware, depicted as a distinct portion of the pie, signifies the growing menace of attacks where cybercriminals encrypt data and demand a ransom for its release. The rising prominence of ransomware underscores the importance of data backup strategies, incident response plans, and proactive cybersecurity measures to prevent and mitigate such attacks.

- Additional segments in the pie chart include exploits, infectors, worms, website defacement, network probing/scanning, each requiring tailored cybersecurity strategies for effective prevention and response.

4. Complementing this, the **bar graph -1 (Figure- 2)** traces the trajectory of cyber threats over a five-year span, from 2018 to 2022. The ascending bars chronicle the relentless increase in the number of reported cyber threats,

providing a visual narrative of the evolving threat landscape. This temporal representation not only underscores the magnitude of the challenge but also enables stakeholders to identify critical inflection points, potential correlations with global events, and patterns that may inform strategic cybersecurity interventions.

5. Combined analysis of **Pie-Chart 4 and Bar graph -1** visually represents a compelling introduction to the intricate relationship between technological progress and the evolving menace of cyber threats in India. The exploration delves into the nuances of each threat category, emphasizing the urgency for proactive cybersecurity measures.

6. The **Bar graph-1** chronicles the escalating trend in cyber threats over the five-year period, providing a visual narrative of the evolving cybersecurity landscape in India. In 2018, the graph initiates with a baseline, representing the reported number of cyber threats at that time. Subsequent bars ascend progressively, signaling a steady increase in the volume and complexity of cyber threats each year.

7. Analysis of Group-2 reports has been tabulated in Table -1. Following analysis has been done:

a. The most common attack vectors/ threats to healthcare industry in India are ransomware and malwares.

b. The expanding dynamics of the cyber-threats have rendered it difficult to specifically derive overall cost of healthcare related breaches which although is not conclusive but rather opens pathway to further research.

c. The IBM report on Cost of a Data Breach published in 2023 supplements the evidence from results of Group 1 Report and Group 2 Reports analysis and that healthcare data breaches and other forms of cyber-threats on the healthcare industry are rapidly increasing.

Table – 1 Analysis of Group 2 reports

Report	Industry	Year	Threat/Attack-vectors
CloudSek	Healthcare/Hospitals	2022	Phishing & BEC DDoS, Ransomware, Insider Threats, Critical Infrastructure, Vulnerabilities/ Exploits
DSCI	Healthcare	2023	Ransomware and Malware
Seqrite	Healthcare	2022	Malware

5. Result and discussion

Upon analysis, unequivocal conclusion can be inferred that CERT-In's is inefficient in reporting cyber-threats and is supported by empirically data. The evidence suggests that CERT-In fails to furnish complete set of details of different forms of cyber-threats, thereby aligning with hypothesis that CERT-In fails to report comprehensive information on cyber-threats. (H_1) In addition to this, the outcome of the analysis also highlights the inadequacies in the reporting mechanism of CERT-In, validating the third hypothesis (H_3). These findings highlight dire inefficiencies within CERT-In's functioning emphasizing the utter need to reformulate the cyber-incident reporting mechanism. In absence of relevant and comprehensive reporting mechanism, stakeholders are ill-equipped to comprehend and respond to cyber-threats efficiently. Hence, taking into consideration the insufficiencies identified in CERT-In's reporting mechanism and is important to improve Indian security posture and ensure protection against developing cyber-threats.

Therefore, addressing the deficiencies identified in CERT-In's reporting practices is imperative to enhance India's cybersecurity posture and safeguard against evolving cyber threats.

Furthermore it is pertinent to note that on October 31, 2023, India witnessed a significant data security breach, marking the largest data breach in the nation's

history. The breach occurred on the Indian Council of Medical Research (ICMR) database led to exposure of sensitive information about over eight hundred fifteen million of the patient's personal records. It should be noted that it was not the only data breach incident, as there were other incidents that occurred earlier this year. The COWIN, a COVID-19 vaccines registry had a breach of confidentiality earlier in the year in June, further contributing to a long line of data security failures. In view of the increasing concern about these occurrences, it is high time that a thorough scrutiny of the incidences and their consequences should be undertaken. Each data breach demonstrates the ever-evolving challenges of today´s data security threats and demands for adequate methods to safeguard sensitive data for businesses in this modern time. The ICMR and COWIN breach incidents act as notable cases that bring to fore certain key considerations. Lack of data on public domain is a critical issue which requires primary attention of the policy makers. Formulation of legal framework and guidelines demonstrate lower efficiency on account of unavailability of concrete and verifiable data. The ongoing increase in cyber-threats only in particular categories is an evidence in itself that no properly defined data has been put forth in past five years. CERT-In being the nodal agency should be vigilant enough to tackle different types of attacks and threats to critical infrastructures like healthcare itself.

6. Suggestions

The reporting system adopted by CERT-In is not full proof and lacks certain provisions. A comparative assessment has been done on CERT-In reporting mechanism with recently proposed U.S. Cyber Incident Reporting for Critical Infrastructure Act of 2022 and European Union's DIRECTIVE (EU) 2022/2555 (NIS Directive 2). A comparative assessment will provide an overview of different aspects which can be adopted by CERT-In to enhance its cyber-incident and cyber security incidents reporting tendency.

	India	U.S.	E.U.	Suggestions
Guiding document	Notification No. 20(3)/2022-CERT-In read with G.S.R. 20(E) (CERT-In. (2022)	Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Committees - H.R.5440 - 117th Congress (2021-2022)	DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (European Union. (2022)	India could consider developing a specific guiding document or regulation focused on cybersecurity reporting in the healthcare sector, similar to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 in the U.S. and Directive (EU) 2022/2555 of the European Parliament and of the Council in the EU
Does Healthcare come under the ambit of Critical Infrastructure	No. (Exception- AIIMS, Delhi)	Yes. (Presidential Policy Directive 21)	Yes. (Annex I - DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL)	India may need to revisit its classification of healthcare as critical infrastructure. While exceptions such as AIIMS, Delhi, are recognized, broader inclusion could enhance cybersecurity preparedness and response across the sector.
Organizations eligible for reporting cyber-threats	Any organization, individual or corporate entity affected by cybersecurity incidents under Annex 1 of No. 20(3)/2022-CERT-In.	- "A covered entity that experiences a covered cyber incident. - A covered entity that makes a ransom payment as the result of a ransomware attack against the covered entity."	Services are provided by: (i) "providers of public electronic communications networks or of publicly available electronic communications services; (ii) trust service providers; (iii) top-level domain name registries and domain name system service providers; (b) the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities; (c) disruption of the service provided by the entity could have a significant impact on public safety, public security or public health; (d) disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact; (e) the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State; (f) the entity is a public administration entity: (i) of central government as defined by a Member State in accordance with national law; or (ii) at regional level as defined by a Member State in accordance with national law that, following a risk-based assessment, provides services the disruption of which could have a significant impact on critical societal or economic activities."	India could establish clear eligibility criteria for reporting cyber threats in the healthcare sector, considering parameters such as the nature of services provided, potential impact on public safety, and significance at the national or regional level.

Timeline (in Hrs)	- As soon as possible in cases of incidents under Annexure I. - 6 hrs in case of other incidents.	72	24– as an early warning. 72 - incident notification	Establishing specific timelines for reporting cyber incidents in the healthcare sector is crucial. India might consider adopting a timeline model similar to the EU's Directive, which mandates reporting within 24 hours for early warning and 72 hours for incident notification.
Types of cyber-incidents should be reported.	Types of cyber security incidents mandatorily to be reported by service providers, intermediaries, data centres, body corporate and Government organisations to CERT-In as provided in Annexure I. **Cyber incident:** "any real or suspected adverse event in relation to cybersecurity that violates an explicitly or implicitly security policy resulting in unauthorized access, denial of service or disruption, unauthorized use of a computer resource for processing or storage of information or changes to data, information without authorization." **Cyber security Incident:** "Any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy, resulting in unauthorized access, denial of service or disruption, unauthorized use of a computer resource for processing or storage of information for changes to data, information without authorization."	Only substantial cyber incident on covered entity- - "Where there is a substantial loss of confidentiality, integrity or availability - Serious impact on the safety and resiliency of operational systems and processes. - A disruption to engage in business or industrial operations, or deliver goods or services - Unauthorized access to information system or network. - Compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or Supply chain compromise."	Any incident that has a significant impact on the provision of services of Member State. (Significant incident).	India should define the types of cyber incidents that healthcare organizations must report. This could include unauthorized access, disruption of services, data breaches, or compromises of critical systems, aligning with definitions provided in other jurisdictions.
Reporting Authority	CERT-In	CISA	Appropriate authority appointed by respective member states	Sub-Division of authority under CISA like 1. Cybersecurity And Infrastructure Security Agency 2. Cybersecurity Division 3. Infrastructure Security Division 4. National Cybersecurity And Communications Integration Center

Whether reporting mandatory?	Yes, for all organizations including protected systems.	By covered entity and in case of significant cyber incident.	For essential and important entities.	A distinguished reporting mechanism for protected systems.
Whether non-compliance punishable?	Yes. Punitive action under section 70B of the IT Act, 2000	Yes. After initial request by Director of Agency, if information still has not be provided to Agency, Subpoena will be issued.	Administrative fine is imposed besides measures under Article 32(4), points (a) to (h), Article 32(5) and Article 33(4). In case of violation of Article 21 or 23, essential entities are subject to administrative fines of a maximum of at least EUR 10 000 000. In case of violation of Article 21 or 23, important entities are subject to administrative fines of a maximum of at least EUR 7 000 000.	Imposition of fine as an initial action may be considered.
Cybersecurity Risk Management	No provision	Provided in NIST Cybersecurity Framework 2.0 (CSF)	Provides for unified approach under Article 21.	A unified and comprehensive risk management framework like NIST CSF may be adopted.

7. Limitations

7.1 Lack of relevant data before establishment of CERT-In

Group 1 and Group 2 reports do not highlight any form of data provided data relating to cyber-threats before 2003. No agency or organization was responsible for recording such incidents. Consequently, there is no benchmark for comparison between recent trends or identify any new patterns forming in the cyberspace.

7.2 Limited literature of industry-wise categorization

The Group 1 and Group 2 reports lack comprehensive categorization of cyber-threat data based on industry. The industry-wise classification is important to understand frequency of such cyber-threats. In absence of such information, it is possible to overlook minute insights into targeted attacks that are healthcare specific. This limits the ability tailor cybersecurity measure to unique challenges faced by different industries.

7.3 Lack of real-time data brings forth challenges to cross-checking of data

The absence of real-time data poses challenges in verifying and cross-checking the accuracy of the information presented in the reports. Real-time data is crucial for staying ahead of rapidly evolving cyber threats. Without it, there may be delays in identifying and responding to emerging threats. Additionally, the inability to cross-check data in real-time hinders the ability to validate the accuracy of reported incidents promptly, potentially impacting the overall effectiveness of cybersecurity measures.

REFERENCES

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. Business Horizons, 62(4), 539–548. https://doi.org/10.1016/j.bushor.2019.03.010

Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 22(2), 177–183. https://doi.org/10.1016/j.eij.2020.07.003

Ibarra, J., Jahankhani, H., & Kendzierskyj, S. (2019). Cyber-physical attacks and the value of healthcare data: Facing an era of cyber extortion and organised crime. In H. Jahankhani, S. Kendzierskyj, A. Jamal, G. Epiphaniou, & H. Al-Khateeb (Eds.), Blockchain and Clinical Trial: Securing Patient Data (pp. 115–137). Springer International Publishing. https://doi.org/10.1007/978-3-030-11289-9_5

Kumar, D. (2023, June 6). AIIMS Delhi hit by fresh cyberattack for second time in a year. Mint. https://www.livemint.com/news/india/aiims-delhi-hit-by-fresh-cyberattacks-details-here-11686061994629.html

Ghosh, S. (2022, November 17). Indian healthcare firms face over 2.78L cyberattacks each month; 2nd to the US. ETCISO; Economic Times. https://ciso.economictimes.indiatimes.com/about_us.php?utm_source=main_menu&utm_medium=newsDetail

Biasin, E. (2020). Healthcare critical infrastructures protection and cybersecurity in the EU: Regulatory challenges and opportunities. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3827114

CERT-In. (2022), Addition of mandated activity. Retrieved from https://www.cert-in.org.in/PDF/Addition_of_Mandated_Activity.pdf

Committees - H.R.5440 - 117th Congress (2021-2022): Cyber Incident Reporting for Critical Infrastructure Act of 2021. (2021, October 1). https://www.congress.gov/bill/117th-congress/house-bill/5440/committees

Cost of Data Breach. (2023a). IBM. https://www.ibm.com/downloads/cas/E3G5JMBP

Cost of Data Breach. (2023b). IBM. https://www.ibm.com/downloads/cas/E3G5JMBP

European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 8 December 2022 on cybersecurity of network and information systems [Eur-Lex Legislation]. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

India Cyber Threat Report. (2023a). Data Security Council of India. https://www.dsci.in/files/content/knowledge-centre/2023/India-Cyber-Threat-Report-2023_0.pdf

India Cyber Threat Report. (2023b). Data Security Council of India. https://www.dsci.in/files/content/knowledge-centre/2023/India-Cyber-Threat-Report-2023_0.pdf

Misra, A., & Chacko, M. (2021). Square pegs, round holes, and Indian cybersecurity laws. International Cybersecurity Law Review, 2(1), 57–64. https://doi.org/10.1365/s43439-021-00026-7

Mittal, A., Saxena , H., & Tripathi , I. (2022a). Increased Cyber Attacks on the Global Healthcare Sector. CloudSek. https://www.cloudsek.com/whitepapers-reports/increased-cyber-attacks-on-the-global-healthcare-sector

Mittal, A., Saxena , H., & Tripathi , I. (2022b). Increased Cyber Attacks on the Global Healthcare Sector. CloudSek. https://www.cloudsek.com/whitepapers-reports/increased-cyber-attacks-on-the-global-healthcare-sector

Quick Heal Annual Threat Report 2022. (2023a). Quick Heal Technologies. https://www.quickheal.co.in/documents/threat-report/quick-heal-annual-threat-report-2023.pdf

Quick Heal Annual Threat Report 2022. (2023b). Quick Heal Technologies. https://www.quickheal.co.in/documents/threat-report/quick-heal-annual-threat-report-2023.pdf

Seqrite annual threat report 2022. (2022a). Retrieved 23 March 2024, from https://www.seqrite.com/seqrite-annual-threat-report-2021#dflip-df_book_full/1/

Seqrite annual threat report 2022. (2022b). Retrieved 23 March 2024, from https://www.seqrite.com/seqrite-annual-threat-report-2021#dflip-df_book_full/1/

Tully, J., Selzer, J., Phillips, J. P., O'Connor, P., & Dameff, C. (2020). Healthcare challenges in the era of cybersecurity. Health Security, 18(3), 228–231. https://doi.org/10.1089/hs.2019.0123

Conflicts Of Interest

The authors declare no conflicts of interest.

Funding

No funding was availed for the purpose of this research.