ORIGINAL RESEARCH PAPER
Volume - 14 | Issue - 09 | September - 2025 | PRINT ISSN No. 2277 - 8179 | DOI : 10.36106/ijsr
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

DIGITAL FRAGILITY IN HEALTHCARE: A COMPARATIVE STUDY OF CYBERSECURITY BREACHES IN INDIA AND GLOBAL HEALTH SYSTEMS (2010–2024)

Hospital Administration

Dr. Sindhu Jonnala* Assistant Professor, Hospital Administration, Govt Medical College/Govt General Hospital Nalgonda *Corresponding Author

Dr. K. Malavika Assistant Professor, Hospital Administration, Govt Medical College/Govt General Hospital Sangareddy

Dr. T. Uday Aditya Assistant Professor, Hospital Administration, Govt Medical College/Govt General Hospital Karimnagar

Dr. C.Narender Kumar Professor & HoD, Hospital Administration, Govt Medical College/Govt General Hospital Quthbullapur

ABSTRACT

Background: Healthcare systems are rapidly digitizing, bringing both efficiency gains and new vulnerabilities. Cybersecurity breaches in hospitals can compromise patient safety, disrupt clinical services, and erode public trust. While global literature on healthcare cyberattacks is growing, India-specific analyses remain sparse. **Objectives:** To document and analyze major cybersecurity incidents in Indian hospitals between 2010 and 2024, compare them with global cases, and identify patterns, systemic vulnerabilities, and lessons for policy and institutional resilience. **Methods:** This cross-sectional analytical descriptive study used secondary data from January 2010 to June 2024. Data sources included media reports, institutional disclosures, government advisories, and cyber forensic analyses. Incidents were coded by year, institution, location, attack type, affected systems, impact, and mitigation measures. A comparative review of high-profile international cases was undertaken to identify cross-context lessons. **Results:** Sixteen major Indian incidents and twelve global cases met inclusion criteria. Ransomware was the most prevalent attack type (56% India; 58% global), frequently targeting Hospital Information Systems (HIS) and Electronic Health Records (EHR). Indian breaches often led to manual operations, diagnostic delays, and underreporting due to lack of mandatory disclosure norms. Global cases demonstrated stronger recovery protocols and regulatory frameworks. **Conclusions:** Cybersecurity in healthcare should be treated as a public health priority. India's increasing reliance on digital health platforms requires immediate reforms, including mandatory breach reporting, cybersecurity accreditation in hospital quality standards, dedicated funding, and integration of cyber-disaster preparedness into health governance.

KEYWORDS

Healthcare cybersecurity, ransomware, hospital information systems, India, global health security, digital health

INTRODUCTION

The digital transformation of healthcare—driven by widespread adoption of Electronic Health Records (EHRs), telemedicine platforms, cloud-based diagnostic tools, and integrated Hospital Information Systems (HIS)—has revolutionized how healthcare is delivered. These innovations enable more efficient patient data management, real-time clinical decision support, remote consultations, and streamlined workflows, ultimately improving accessibility, quality, and continuity of care. Particularly in resource-constrained settings, digital health technologies hold promises to bridge gaps in healthcare delivery and expand reach to underserved populations.

However, the rapid integration of digital infrastructure also introduces critical systemic vulnerabilities. Healthcare data systems have become prime targets for cyberattacks, including ransomware, phishing, malware, distributed denial of service (DDoS), insider threats, and large-scale data breaches. Unlike many other sectors, healthcare faces unique risks: patient safety is directly tied to the availability and integrity of clinical data and hospital systems, where interruptions or data loss can lead to delayed diagnoses, medication errors, compromised treatment plans, and in extreme cases, patient mortality. Moreover, healthcare institutions often manage vast volumes of sensitive personal health information, making them attractive targets for financially motivated cybercriminals and hostile actors.

Globally, the frequency and sophistication of cyberattacks on healthcare have escalated sharply in recent years, exposing gaps in preparedness and resilience even in high-income countries. The 2017 Wanna Cry ransomware attack disrupted operations across 81 NHS trusts in the United Kingdom, forcing cancellation of thousands of appointments and surgeries, and highlighting the vulnerability of critical infrastructure. Similarly, the 2021 Conti ransomware attack on Ireland's Health Service Executive (HSE) brought the nation's health services to a standstill for weeks, demonstrating how cyber incidents can paralyze public health systems and erode public trust.

India, amidst its ongoing digital health expansion under initiatives like Ayushman Bharat Digital Mission and National Digital Health Blueprint, faces similar and distinct cybersecurity challenges. The 2022 ransomware attack on AIIMS Delhi, one of the country's largest tertiary care centers, disrupted hospital operations for over two weeks and compromised access to over 40 million patient records. Such incidents underline the growing threat landscape in Indian healthcare—a sector marked by heterogeneous IT infrastructure, limited cybersecurity staffing, and regulatory gaps. Despite increasing digitization, healthcare cybersecurity remains a relatively nascent and under-researched area in India, with limited public reporting and few enforced policies on breach notification and data protection.

This backdrop necessitates a comprehensive examination of healthcare cybersecurity breaches in India, to understand their nature, impact, and systemic vulnerabilities. By situating Indian incidents within the broader global context, this study aims to identify actionable insights that can inform institutional readiness and policy frameworks. Strengthening cybersecurity in Indian healthcare is critical not only for protecting patient data and ensuring service continuity but also for sustaining public confidence in the country's digital health transformation.

Objectives:

1. Document and categorize major cybersecurity incidents in Indian hospitals (2010–2024).
2. Analyse the typology, vectors, and affected systems.
3. Assess clinical and operational impacts.
4. Compare Indian incidents with global cases to identify lessons.

2. METHODS

2.1 Study Design

Cross-sectional, analytical descriptive study using secondary data.

2.2 Data Sources

- National and international news reports
- Hospital, health ministry, and CERT-In disclosures
- Cybersecurity advisories (CISA, MITRE)
- Grey literature, technical blogs, and forensic reports

2.3 Inclusion Criteria

Criterion	Description
Timeframe	Jan 2010 – Jun 2024

Sector	Hospitals (≥100 inpatient beds), insurers, diagnostics directly linked to patient care
Impact	Tangible operational disruption, data compromise, or clinical risk
Verification	At least one official or widely recognized source

2.4 Exclusion Criteria
- Attacks on small clinics or standalone diagnostic centers
- Unverified social media claims

2.5 Variables Coded
- Year & Institution
- Location
- Type of Attack (ransomware, phishing, DDoS, etc.)
- Systems Affected
- Operational & Clinical Impact
- Mitigation Measures

2.6 Comparative Analysis
Selected global incidents were analyzed for attack type, scale, and response strategies.

Ethical Considerations: All data were from publicly available sources; no patient-identifiable information was accessed.

3. RESULTS
3.1 Overview
A total of 28 major healthcare cybersecurity incidents were analysed in this study, comprising 16 incidents from India and 12 from global contexts. These cases were carefully selected based on their impact, scale, and availability of verified information, and are systematically presented in Table 1 and Table 2 respectively.

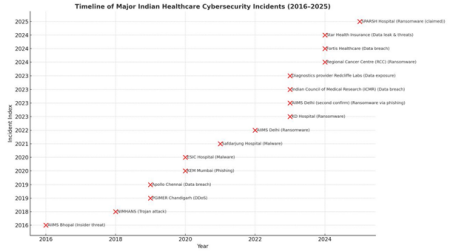

Figure 1 — a clear timeline of major Indian healthcare cybersecurity incidents from 2016 to 2025, showing each event chronologically with labelled institutions

Table 1. Indian Healthcare Cybersecurity Incidents, 2016–2025

Year	Institution	Location	Type of Attack	System Affected	Impact
2016	AIIMS Bhopal	Bhopal	Insider threat	Lab MIS	Misdiagnosis cases reported
2018	NIMHANS	Bengaluru	Trojan attack	Research data servers	Research halt
2019	PGIMER Chandigarh	Chandigarh	DDoS	Hospital website	Appointment system affected
2019	Apollo Chennai	Chennai	Data breach	Cloud-based EHR	2000 patient records leaked
2020	KEM Mumbai	Mumbai	Phishing	Email server	Minimal
2020	ESIC Hospital	Hyderabad	Malware	Payroll and billing	Staff salaries delayed
2021	Safdarjung Hospital	Delhi	Malware	PACS (Radiology)	Diagnostic delays
2022	AIIMS Delhi	New Delhi	Ransomware	HIS, EHR	40M+ records inaccessible
2023	KD Hospital	Ahmedabad (Gujrat)	Ransomware	Online systems, CCTV, patient files	Server encryption, $70k ransom demand; operations manually restored
2023	AIIMS Delhi (second confirm)	New Delhi	Ransomware via phishing	HIS / e-hospital service	Encrypted OPD systems; ₹200 cr demand; manual mode for ~2 weeks
2023	Indian Council of Medical Research (ICMR)	Pan-India	Data breach	COVID-19 testing database	Leaked personal data of ~81.5 crore individuals
2023	Diagnostics provider Redcliffe Labs	Bengaluru	Data exposure	Patient test results database	12M records exposed in open database
2024	Regional Cancer Centre (RCC)	Thiruvananthapuram, Kerala	Ransomware	Radiation & patient data servers	5-day disruption; ransom demand $100M; data intact via backups
2024	Fortis Healthcare	Multiple cities	Data breach	Patient data systems	Alleged theft of extensive patient records by "Kill Security"
2024	Star Health Insurance	Chennai (insurer HQ)	Data leak & threats	Policyholder records	7.24 TB data leaked affecting 31M; death threats sent to execs
2025	SPARSH Hospital	Bangalore	Ransomware (claimed)	Hospital website	Attack claimed by KillSec; technical hash shared

The Indian incidents reflect a diverse array of cyber threats targeting various hospital systems, including ransomware attacks on Hospital Information Systems (HIS), data breaches involving patient records, insider threats, and malware infections affecting critical diagnostic and administrative platforms.

The global incidents, drawn from high-income and middle-income countries, provide a comparative framework illustrating common attack vectors such as ransomware and supply chain exploits, as well as differing response strategies and recovery outcomes. This dual perspective allows for a comprehensive understanding of the evolving threat landscape, operational impacts, and resilience measures within Indian healthcare institutions relative to international experiences.

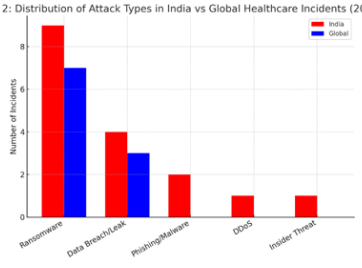

Figure 2: Distribution of attack types in India vs Global, a side-by-side comparison showing that ransomware dominates both Indian and global healthcare cyber incidents, while India reports a more varied mix including phishing, malware, DDoS, and insider threats.

Table 2. Selected Global Healthcare Cybersecurity Incidents, 2017–2025

Year	Institution	Country	Type of Attack	System Affected	Impact
2017	NHS (WannaCry)	UK	Ransomware (WannaCry)	IT systems, EHRs	81 NHS trusts hit; 19,000 appointments cancelled
2019	LifeLabs	Canada	Ransomware & Data Theft	Lab systems	Data of 15M Canadians exposed; ransom paid
2021	HSE Ireland	Ireland	Ransomware (Conti)	All IT systems	Complete shutdown; 520 patient records leaked
2021	Waikato DHB	New Zealand	Ransomware	All digital services	Surgery cancellations; staff resorted to paper records
2022	Medibank	Australia	Data Breach (REvil-linked)	Customer & health records	9.7M users affected; no ransom paid

PRINT ISSN No. 2277 - 8179 | DOI : 10.36106/ijsr

2023	MOVEit breach	Global	Supply Chain Exploit	Secure file transfer service	2,700+ orgs affected; 93M+ records exposed
2024	Change Healthcare	USA	Ransomware (ALPHV)	Billing, claims, eRx systems	$22M ransom paid; billing/prescription delays across US
2024	Ascension Health	USA	Ransomware	EHR, diagnostics, operations	140 hospitals impacted; 37-day downtime; $130M cost
2024	Synnovis (NHS)	UK	Ransomware (Qilin)	Pathology systems	Blood tests & surgeries delayed; 400GB NHS data stolen
2024	Lurie Children's Hospital	USA	Ransomware (Rhysida)	Patient records	791,000 records leaked after non-payment of $3.7M ransom
2025	Frederick Health	USA	Ransomware	Personal & clinical data	934,000 patients affected; credit monitoring offered
2025	Kettering Health	USA	Undisclosed (suspected)	Network-wide systems	Emergency reroutes across all hospitals

3.2 Patterns Observed
- **Rise Post-2018:** Coinciding with accelerated EHR adoption.
- **Predominance Of Ransomware:** Affecting HIS, EHR, and PACS systems.
- **Operational Disruption:** Downtime from hours to >30 days.
- **Underreporting In India:** Lack of mandatory disclosure norms delays public awareness.

3.3 Comparative Insights
- **Global** cases had more robust recovery plans, coordinated responses, and transparent communication.
- **Indian** institutions relied on manual operations, with recovery often supported by external vendors or CERT-In.

DISCUSSION
4.1 Cybersecurity As A Public Health Threat
Cybersecurity breaches in healthcare represent a critical and often underestimated public health threat. Hospital Information Systems (HIS), Electronic Health Records (EHR), and diagnostic platforms are foundational to modern clinical workflows, supporting everything from patient registration and medical history tracking to laboratory diagnostics, radiology imaging, medication management, and care coordination. Disruptions to these systems, whether due to ransomware attacks, malware infiltration, or denial-of-service assaults, have immediate and tangible impacts on patient care delivery.

Even brief outages can delay vital diagnostic procedures, postponing the identification and treatment of acute and chronic conditions. For example, the inability to access EHRs can prevent clinicians from reviewing allergy information, lab results, or medication histories, increasing the risk of adverse drug reactions or medical errors. Interruptions in electronic prescribing systems may delay critical medications, while compromised diagnostic platforms can hinder timely imaging or pathology services, directly affecting treatment decisions.

Beyond operational delays, cybersecurity incidents elevate clinical risk by forcing healthcare providers to revert to manual, paper-based processes that are prone to errors and inefficiencies. These fallback methods often lack the real-time data integration necessary for complex decision-making and may overwhelm staff already burdened by clinical workloads. In emergency and intensive care settings, such disruptions can exacerbate patient morbidity and mortality.

Moreover, breaches involving the theft or manipulation of patient data undermine trust in healthcare institutions, discouraging individuals from sharing sensitive information essential for effective care. Large-scale data leaks can lead to identity theft, insurance fraud, and stigmatization, further affecting patients' willingness to seek timely medical attention.

The public health implications extend beyond individual facilities. Cyberattacks that disable multiple hospitals or regional health networks can disrupt broader health service delivery, compromise public health surveillance systems, and hinder responses to epidemics or disasters. For instance, delays in reporting notifiable diseases or interruptions in telemedicine services can affect entire populations, especially vulnerable groups with limited healthcare access.

Given these wide-ranging consequences, cybersecurity in healthcare must be recognized not just as an IT issue but as a fundamental component of patient safety and public health. Strengthening cybersecurity resilience is essential to safeguard clinical outcomes, maintain continuous care delivery, protect sensitive health information, and preserve public trust in the healthcare system.

4.2 Systemic Vulnerabilities In India
Indian public hospitals operate within a complex environment characterized by a convergence of technological, infrastructural, and operational weaknesses that significantly increase their susceptibility to cybersecurity threats. These systemic vulnerabilities hinder effective prevention, detection, and response to cyberattacks, exposing critical healthcare services and sensitive patient data to risk. Key challenges include:
- **Unpatched Legacy Systems:** Many public healthcare institutions continue to rely on outdated hardware and software systems that are no longer supported by vendors or incompatible with modern security protocols. These legacy systems often lack the capability to receive critical security patches or updates, creating exploitable gaps that attackers can leverage. The difficulty and cost of migrating to newer platforms exacerbate this issue, prolonging exposure to known vulnerabilities.
- **Weak Endpoint Protection:** Devices used across hospital networks—such as computers, diagnostic machines, and IoT-enabled equipment—often lack robust endpoint security measures. Insufficient antivirus, firewall protections, and intrusion detection systems leave these endpoints vulnerable to malware, ransomware, and unauthorized access. In many cases, endpoint security software is outdated, improperly configured, or absent altogether.
- **Low Staff Awareness and Training:** Human factors remain a major vulnerability in healthcare cybersecurity. A significant proportion of hospital staff, including clinicians and administrative personnel, lack adequate training on recognizing phishing attempts, social engineering tactics, and safe digital practices. This gap increases the likelihood of successful attacks initiated through deceptive emails, malicious links, or compromised credentials. The absence of ongoing cybersecurity awareness programs leaves staff ill-prepared to identify or respond effectively to evolving threats.
- **Absence of Dedicated Cybersecurity Personnel:** Unlike many private sector organizations, most Indian public hospitals do not employ full-time cybersecurity professionals or Chief Information Security Officers (CISOs) with clearly defined responsibilities for overseeing security governance. The lack of specialized personnel hampers the development and enforcement of security policies, incident monitoring, threat intelligence integration, and rapid response capabilities. Cybersecurity duties, when assigned, are often secondary roles performed by general IT staff with limited training.

Together, these factors create a fragile cybersecurity posture within India's public healthcare system, increasing operational risks and potential harm to patients. Addressing these vulnerabilities requires a strategic focus on modernizing infrastructure, investing in endpoint protection technologies, fostering a culture of cybersecurity awareness, and institutionalizing specialized security roles across hospitals.

4.3 Policy And Regulatory Gaps
India's healthcare cybersecurity landscape is further challenged by significant policy and regulatory shortcomings, especially when compared to established frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States or the General Data Protection Regulation (GDPR) in the European Union. These international standards impose stringent requirements for data protection, breach notification, and accountability, fostering transparency and enabling systemic improvements.

In contrast, India currently lacks a dedicated and comprehensive

breach notification mandate specific to the healthcare sector. Although the Digital Personal Data Protection Act and Information Technology Act provide some data privacy provisions, there is no enforceable requirement compelling healthcare institutions to promptly disclose cybersecurity incidents. This absence of mandatory reporting creates a regulatory blind spot, resulting in underreporting or delayed disclosure of breaches.

The lack of transparency undermines public trust and impedes timely interventions by regulators and cybersecurity agencies. Without consistent and standardized incident reporting, it becomes difficult to identify common vulnerabilities, assess emerging threat trends, or develop targeted prevention strategies across the sector. Moreover, this regulatory gap diminishes accountability, as healthcare organizations may lack incentives to prioritize cybersecurity investments or adhere to best practices in the absence of legal consequences for breaches.

The missed opportunity for coordinated responses at national or regional levels further compounds risks. Effective cybersecurity requires collaboration among hospitals, government bodies, and CERTs (Computer Emergency Response Teams) to share threat intelligence, conduct joint investigations, and rapidly contain attacks. Without policy-driven mandates, such collective mechanisms remain fragmented or underutilized.

Addressing these gaps through robust, healthcare-specific regulations—including clear breach notification requirements, compliance audits, and enforcement provisions—will be critical to enhancing India's healthcare cybersecurity resilience. Regulatory reform can drive a culture of accountability and continuous improvement, ultimately safeguarding patient data and ensuring uninterrupted healthcare delivery.

4.4 Lessons From Global Cases

International experience with healthcare cybersecurity breaches offers valuable lessons that can inform and strengthen India's response to this growing threat. Several critical strategies have emerged from countries with advanced digital health systems, underscoring best practices in institutional preparedness, response coordination, and resilience building.

- **Preparedness Drills and Cyber-Disaster Simulations:** The UK's National Health Service (NHS) and Ireland's Health Service Executive (HSE) have institutionalized regular cybersecurity drills and simulated attack scenarios. These exercises test system robustness, response protocols, and staff readiness, allowing organizations to identify vulnerabilities before actual incidents occur. Such proactive preparedness significantly enhances institutional resilience and reduces recovery times when breaches do happen.
- **Rapid, Coordinated Government Response And Clear Patient Communication:** Timely intervention by government agencies, coupled with transparent communication to patients and the public, helps mitigate both operational disruptions and reputational damage. Clear messaging reassures stakeholders, maintains trust, and facilitates collaboration between healthcare providers, cybersecurity teams, and law enforcement.
- **Segmented IT Networks and Secure Offline Backups:** Implementing network segmentation limits the lateral movement of attackers within hospital IT infrastructures, containing breaches to isolated systems rather than allowing widespread infection. Maintaining secure, offline backups ensures that critical data and systems can be restored promptly without succumbing to ransom demands or data loss.

The rising frequency and sophistication of cyberattacks on hospitals underscore a critical intersection between patient safety and digital resilience. Unlike other sectors where breaches primarily affect financial or reputational standing, healthcare cyber incidents can directly compromise clinical outcomes. Even short-term system outages may delay diagnoses, interrupt treatment regimens, and, in severe cases, lead to preventable morbidity or mortality.

The 2022 ransomware attack on AIIMS Delhi, which incapacitated one of India's largest tertiary care hospitals for over two weeks, exemplifies how the heavy reliance on interconnected IT systems magnifies operational vulnerabilities. Similarly, global incidents such as the 2020 cyberattack on Dusseldorf University Hospital in Germany—linked to a ransomware infection that contributed to the death of a patient due to delayed emergency care—highlight the life-threatening potential of healthcare cybersecurity failures.

Despite technological advances in encryption, access control, and AI-driven threat detection, systemic challenges remain pervasive, especially in resource-limited public hospitals. Outdated infrastructure, insufficient cybersecurity training, and weak policy enforcement continue to expose critical systems to attack. Addressing these challenges requires **a dual-pronged approach** that combines robust technical safeguards—such as continuous monitoring, threat intelligence integration, and resilient system architecture—with governance reforms that foster a culture of cybersecurity awareness and accountability at all levels of healthcare delivery. Only through such comprehensive efforts can healthcare institutions effectively safeguard patient safety in an increasingly digital world.

4.5 Recommendations

1. **Mandatory Breach Reporting:** Enforce compulsory incident disclosure under India's Digital Personal Data Protection Act to ensure transparency, accountability, and sector-wide learning from cybersecurity events.
2. **Dedicated Funding And Personnel:** Establish earmarked annual IT and cybersecurity budgets within hospital financial planning, covering system upgrades, licensed security software, and infrastructure hardening.
3. **Specialised Hiring:** Recruit full-time Chief Information Security Officers (CISOs) and hospital IT security teams, with defined roles for network security, incident response, and compliance monitoring.
4. **Standard Operating Procedures (SOPs) For Safe Access:** Develop and enforce hospital-wide SOPs governing secure access to HIS, EHR, and diagnostic platforms, including role-based permissions, multi-factor authentication, and regular access audits.
5. **Integration Into Accreditation:** Embed detailed cybersecurity standards and compliance checks into NABH and NQAS accreditation frameworks, making digital safety an essential quality parameter.
6. **Annual Audits And Simulations:** Conduct independent cyber-audits and regular simulation exercises to test system resilience and staff readiness under realistic attack scenarios.
7. **Capacity Building**: Implement ongoing staff training programmes focused on phishing awareness, secure data handling, and rapid reporting of suspicious activities.

Limitations

- Based solely on publicly available data — actual incident numbers likely higher.
- Incomplete technical details limited root cause analysis.
- Variation in institutional transparency.

CONCLUSION

Cybersecurity breaches in healthcare pose a profound threat not only to patient safety but also to the operational integrity and public trust of healthcare institutions. As India rapidly expands its digital health ecosystem through initiatives like the National Digital Health Mission and widespread adoption of Electronic Health Records, the sector faces an urgent imperative to strengthen its cybersecurity posture. Without timely and coordinated action, vulnerabilities in infrastructure, workforce preparedness, and regulatory frameworks will continue to expose hospitals and patients to significant risks.

Safeguarding healthcare in the digital age requires a holistic approach that integrates advanced technical safeguards—such as robust endpoint security, network segmentation, and resilient backup systems—with comprehensive institutional preparedness, including dedicated cybersecurity personnel, staff training, and incident response planning. Equally critical is the establishment of clear and enforceable policy frameworks that mandate breach reporting, define accountability, and foster transparency.

By elevating healthcare cybersecurity to the level of a public health priority, India can ensure the continuity and safety of clinical services, protect sensitive patient data, and sustain public confidence in its health systems. Structured governance, sustained funding, and proactive regulatory oversight are essential pillars in this endeavour. Only through such concerted efforts can the promise of digital health transformation be fully realized—delivering safer, more efficient, and

equitable care for all.

REFERENCES

1. New Indian Express. AIIMS Delhi held to ransom by cyber attack. New Indian Express [Internet]. 2022 Nov 28 [cited 2025 Aug 10]. Available from: The New Indian Express
2. Cyber Management Alliance. AIIMS ransomware attack – Cyber-attack forces manual operations. Cyber Management Alliance [Internet]. 2024 [cited 2025 Aug 10]. Available from: CM Alliance
3. Mint. AIIMS Delhi hit by fresh cyberattack for second time in a year. Mint [Internet]. 2023 [cited 2025 Aug 10]. Available from: mint
4. IGI (Youth Ki Awaaz). On KD Hospital ransomware attack: A security researcher's perspective. Youth Ki Awaaz [Internet]. 2023 Nov [cited 2025 Aug 10]. Available from: Youth Ki AwaazBPAS Journals
5. Indian Express. Hospital falls prey to ransomware attack, hackers demand $70,000. Indian Express [Internet]. 2023 May [cited 2025 Aug 10]. Available from: The Indian ExpressDeshGujarat
6. TechInformed. ICMR data breach one of largest in India's history. TechInformed [Internet]. 2023 Oct 31 [cited 2025 Aug 10]. Available from: TechInformed
7. The Cyber Express. 12 Million Redcliffe Labs Records with PII Found Exposed. The Cyber Express [Internet]. 2023 Oct [cited 2025 Aug 10]. Available from: The Cyber ExpressThe Financial Express
8. UNI India. RCC cyberattack: Ransom in cryptocurrency demanded, 20 lakh patient data stolen. UNI India [Internet]. 2024 May 8 [cited 2025 Aug 10]. Available from: Uniindia
9. New Indian Express. Probe says Russian hackers behind cyber attack in Thiruvananthapuram Regional Cancer Centre. New Indian Express [Internet]. 2024 Jun 8 [cited 2025 Aug 10]. Available from: The New Indian ExpressKerala Kaumudi
10. CyberPress. Hackers Allegedly Claiming breach of Fortis Healthcare Data. CyberPress [Internet]. 2024 Oct [cited 2025 Aug 10]. Available from: Cyber Security News
11. Reuters. Hacker uses Telegram chatbots to leak data of top Indian insurer Star Health. Reuters [Internet]. 2024 Sep 20 [cited 2025 Aug 10]. Available from: Reuters
12. Reuters. India's Star Health absolves security chief in data leak incident. Reuters [Internet]. 2024 Oct 28 [cited 2025 Aug 10]. Available from: Reuters
13. Reuters. Star Health insurer sues Telegram after hacker uses app's chatbots to leak data. Reuters [Internet]. 2024 Sep 26 [cited 2025 Aug 10]. Available from: Reuters
14. Reuters. Star Health hacker says death threats and bullets sent to executives. Reuters [Internet]. 2025 May 9 [cited 2025 Aug 10]. Available from: ReutersThe Times of India
15. Economic Times (ManageEngine Insights). How the Star Health breach impacts trust in India's digital health. ManageEngine Insights [Internet]. 2024 Oct [cited 2025 Aug 10]. Available from: ManageEngine Insights
16. Sparsh Hospital Bengaluru claimed ransomware 2025. The Economic Times [Internet]. 2025 [cited 2025 Aug 10]
17. Smith RD, Woodall J, Kelly G, et al. A retrospective impact analysis of the WannaCry cyber-attack on the English NHS. BMJ Open [Internet]. 2019 May;9(5):e027859. DOI:10.1136/bmjopen-2018-027859. [cited 2025 Aug 10]. Available from: The Indian Expres
18. LifeLabs ransomware Canada 2019. CBC News [Internet]. 2019 [cited 2025 Aug 10].
19. SE Ireland Conti ransomware 2021. The Guardian [Internet]. 2021 [cited 2025 Aug 10]
20. Waikato DHB New Zealand ransomware 2021. New Zealand Herald [Internet]. 2021 [cited 2025 Aug 10].
21. Medibank Australia data breach 2022. Sydney Morning Herald [Internet]. 2022 [cited 2025 Aug 10]
22. MOVEit breach 2023 supply chain global. Reuters [Internet]. 2023 [cited 2025 Aug 10].
23. Change Healthcare USA ALPHV ransomware 2024. Bloomberg [Internet]. 2024 [cited 2025 Aug 10]
24. Ascension Health USA ransomware 2024. Dallas Morning News [Internet]. 2024 [cited 2025 Aug 10].
25. Synnovis (NHS) Qilin ransomware 2024. Financial Times [Internet]. 2024 [cited 2025 Aug 10]
26. Lurie Children's Hospital USA Rhysida ransomware 2024. Chicago Tribune [Internet]. 2024 [cited 2025 Aug 10].
27. Frederick Health USA ransomware 2025. Local News [Internet]. 2025 [cited 2025 Aug 10].
28. Kettering Health USA 2025 suspected ransomware. USA Today [Internet]. 2025 [cited 2025 Aug 10].