



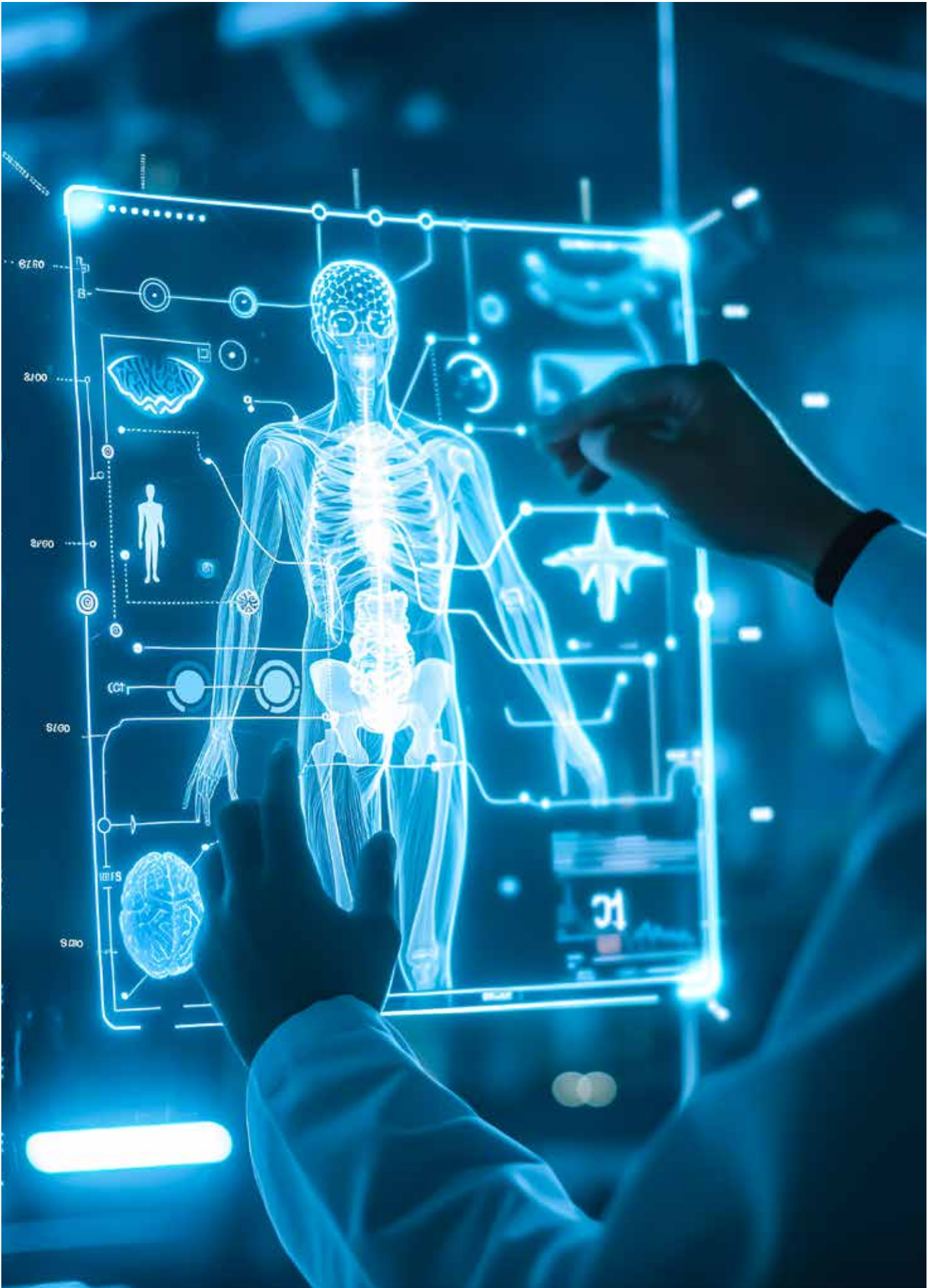
Cyber resilience in hospitals:

Safeguarding India's
healthcare industry
in the digital age

November 2024

Table of contents

Foreword	03
Indian hospitals' perspective: Evolution of hospitals through digital transformation	04
Healthcare's digital shift through cloud migration in hospitals	08
Exploring the dynamic landscape of healthcare: The hospital ecosystem in India	09
Unlocking potential: The crucial role of digitisation in public healthcare	10
Indian hospitals' perspective: Cybersecurity challenges and solutions	11
Impact of digital transformation and pandemic: Challenges, threats and vulnerabilities	12
Security investments, priorities, and Security Operations Centre (SOC) in hospitals	14
Use of SOC in hospitals	15
Tools and technologies used by leading hospitals	16
Security and privacy governance in hospitals	17
Strategic cybersecurity: Board and management involvement in cyberspace	18
Hospitals and their key pillars of resilience	19
Way ahead and conclusion	21
Key takeaways	22
Conclusion	22
Connect with us	23



Foreword

India has a long history and legacy of healthcare services. In the ancient period, pioneers such as *Sushruta* and *Charaka* established a comprehensive ecosystem of hospitals where surgeries and medicines were provided.

The start of modern hospitals in India can be traced back to 1664 when the Madras General Hospital was set up. We have come a long way since then. Today, the average Indian household spends about 5.9 percent¹ of its annual expenditure on health. This number has doubled since 2012. Therefore, consumer awareness and commitment to health have increased in the last 10 years. Correspondingly, there has been increased investment in both public and private healthcare.

In the 2024 interim budget² the government has allocated INR 90,171 crore to healthcare this year, marking an almost 14 percent increase from last year's allocation. Similarly, there has been a significant increase in growth within the private healthcare system. Presently valued at US\$66 billion, the private healthcare system is expected to surpass US\$100 billion by 2027.³

Over the past five years, there has been an unprecedented adoption of digital technologies in the healthcare system. Key areas of transformation include patient engagement and experience, clinical data lakes, clinical decision support systems, operational efficiency and new care models such as telemedicine. This transformation is delivered via the cloud, contributing to the higher adoption of cloud technology in healthcare compared with the life sciences sector.

As a result of the increased digital footprint, cyber-attacks on the healthcare sector have risen. Today, India ranks among the world's top five most cyber-attacked healthcare systems.⁴ These attacks have prompted a strategic shift in the mindset of top management, leading to a significant increase in cyber investments within the healthcare industry.

Per our analysis, cybersecurity budgets now account for approximately 8–10 percent of the overall IT budget, marking

a positive development. Additionally, considerable efforts are being made at the executive management level of hospitals and within the board to raise awareness about cyber issues across hospitals.

In this report, we have examined the evolution of hospitals and the ongoing transformation in hospitals driven by digital technologies. This includes not only the adoption of advanced patient management systems but also the implementation of Clinical Decision Support Systems (CDSS), patient bots, cognitive technologies and GenAI. These critical investments aim to enhance patient care, streamline operations and improve healthcare outcomes.

This report explores the cybersecurity challenges in healthcare, discussing investments, top priorities and the tools and technologies essential for safeguarding healthcare data. With hospitals now relying more on digital platforms and interconnected systems, they are increasingly susceptible to cyber threats. Therefore, understanding security governance and strategic initiatives is crucial for resilience against these risks.

We extend our heartfelt gratitude to the healthcare industry experts for their valuable contributions to this report, dedicating their time and insights. We trust that you will find the report beneficial, and it will assist you in your cybersecurity endeavours.

Regards,



Vinayak Godse
CEO,
Data Security Council
of India (DSCI)



Deepa Seshadri
Partner & Leader - Cyber
Deloitte South Asia

¹ Household Consumption Expenditure Survey (HCES), Ministry of Statistics and Programme Implementation, 2022-2023; https://www.mospi.gov.in/sites/default/files/publication_reports/Factsheet_HCES_2022-23.pdf?download=1

² Budget 2024 Announcements Impact and Highlights Updates, The Economic Times, 02 February 2024; <https://economictimes.indiatimes.com/news/newsblogs/budget-2024-news-live-announcements-impact-highlights-updates-2-feb-2024/liveblog/107338900.cms>

³ Critical state of healthcare: India had 2nd highest number of cyber attacks in the world in 2021, CNBC TV18, 03 September 2022; <https://www.cnbcvtv18.com/information-technology/indian-healthcare-industry-records-second-highest-cyberattacks-globally-14638171.htm>

⁴ Critical state of healthcare: India had 2nd highest number of cyber attacks in the world in 2021, CNBC TV18, 03 September 2022; <https://www.cnbcvtv18.com/information-technology/indian-healthcare-industry-records-second-highest-cyberattacks-globally-14638171.htm>



Indian hospitals' perspective: Evolution of hospitals through digital transformation

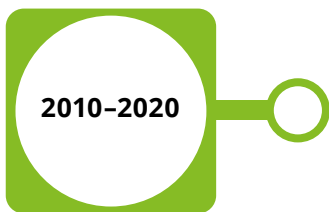
Over the past few decades, India has significantly improved health indicators such as immunisation rates, life expectancy and mortality rates. While substantial progress has been made in eradicating smallpox and polio, India continues to set higher targets. A notable example of successful public-private collaboration is evident in our efforts to eliminate tuberculosis using a combination of emerging technologies, including AI.

Private hospitals in India initially focused on providing specialised tertiary and quaternary care, particularly in general medicine and surgery. Today, almost 30 percent of the specialised services in hospitals are in the cardiology therapeutic area, closely followed by orthopaedics. Over the last five years, oncology has emerged as the fastest-growing

therapeutic area, reflecting a significant shift from mere procedures to holistic wellness.

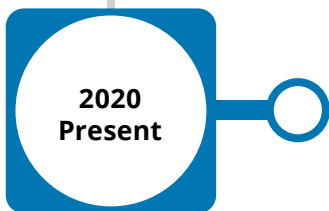
The COVID-19 pandemic further accelerated the enhancement of the hospital's digital infrastructure. The pandemic prompted the release of guidelines for telemedicine, leading to a further expansion of the digital footprint in healthcare. The usage of digital technology within the healthcare sector has been expedited, and emerging technologies are facilitating the advancement of cost-effective, superior therapeutic interventions. Subsequent strategies must focus on assisting India in developing a digitally advanced and enduring healthcare infrastructure for the future.

Here are some key highlights of the evolving scenarios:



This era witnessed the initial adoption of technology by most hospitals, characterised by:

- Development of custom-built software for billing and financials.
- Basic Health Information Systems (HIS), either developed in-house or as part of Corporate Social Responsibility (CSR) initiatives by major global IT firms.
- Initial adoption of document management systems.



Clinical technology for operational efficiency

- For a significant period, key technology investments in hospitals focused on diagnostic equipment such as Computed Tomography (CT) scans, Magnetic Resonance Imaging (MRI) and X-rays.
- Over the past five years, there has been a significant increase in investments in other areas, such as digital pathology, robotic surgery equipment and Artificial Intelligence (AI) for CDSS.
- Nowadays, almost all major corporate hospitals use a digital Health Management Information System (HMIS), although many are on-premises, primarily to enhance security and reduce storage costs. Approximately 13 percent of the private healthcare system is dominated by large chains or corporate hospitals.



Patient experience

- Many hospitals invest in patient management systems that streamline workflow and improve patient experience.
- Critical investments have been made in CRM systems, patient bots, cognitive technologies and GenAI.

2020 Present



New care models

- Hospitals have started investing in improving diagnostics over the next 5–10 years using technologies such as remote monitoring, AI-enabled diagnosis and Internet of Things (IoT) devices.
- Chronic care management and using at-home healthcare or 'hospitals without walls' are other concepts being developed.



Vertical integrations and extensions of the business

- Mergers and acquisitions of smaller chains by larger healthcare chains, advancements in cost-effective therapies in genetic-based research and immunotherapies.
- Mid to large-scale hospitals are investing Capital Expenditure (CapEx) in practices such as oncology, robotic surgery, IVF setups, etc., focusing on customer experience and building a multiverse of solutions incorporating healthcare by designing multi-speciality clinics, pharmacies, secondary care and women and child therapies.

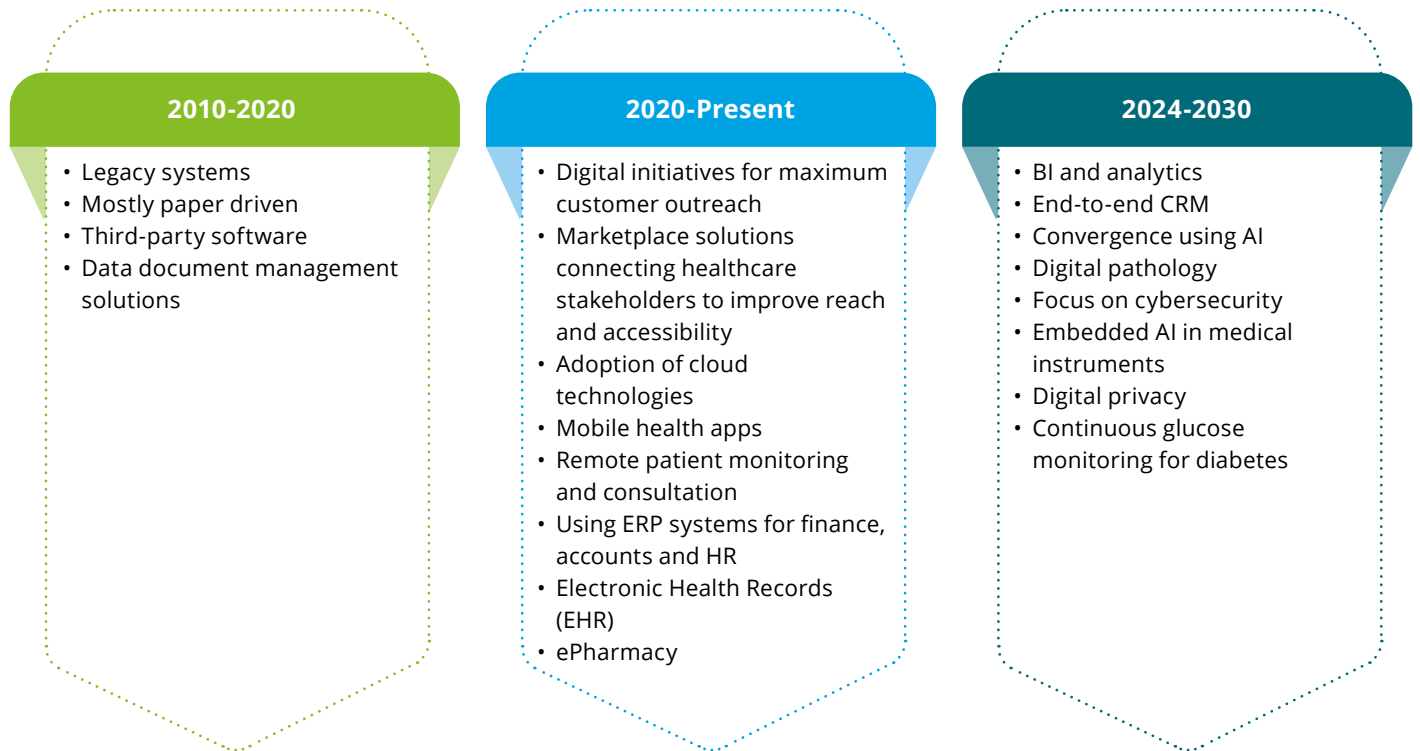
2024–2030 Predictions

In the next six years, we will see enhanced development in the following key areas:

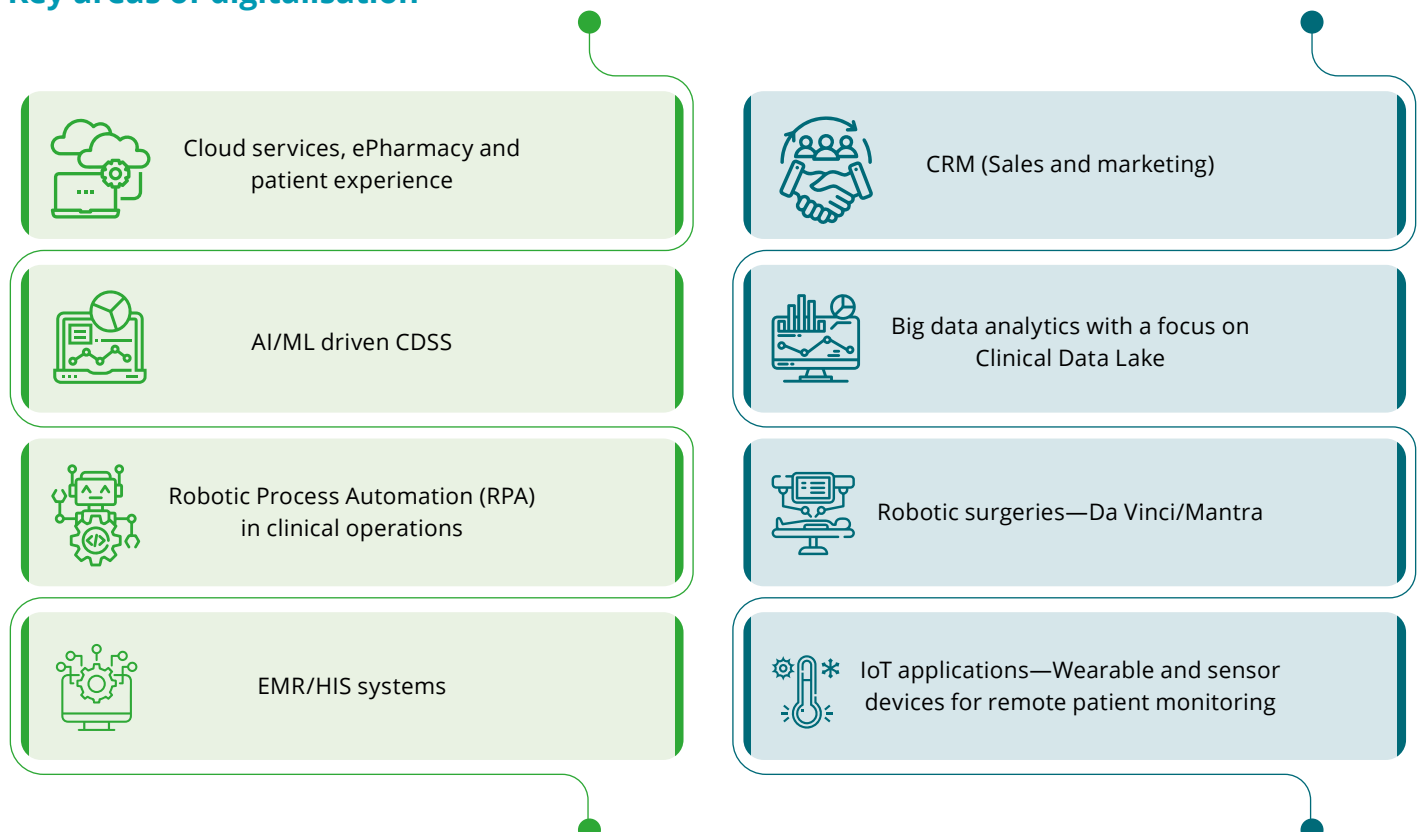
- Integration of HIS and EMR systems with government programmes such as Ayushman Bharat Digital Health Mission.
- Interoperable patient records, where the records can be shared with various providers based on a consent mechanism.
- Integration of AI into clinical diagnosis and enhanced remote diagnosis of patients.
- Molecular biology and genomic research for personalised therapy and medicines.
- Clinical boards will be established for all major therapeutic areas.
- Enhanced digital transformation in key areas.



These advancements are underpinned by robust investments in cybersecurity and data privacy, which will be explored in this report.

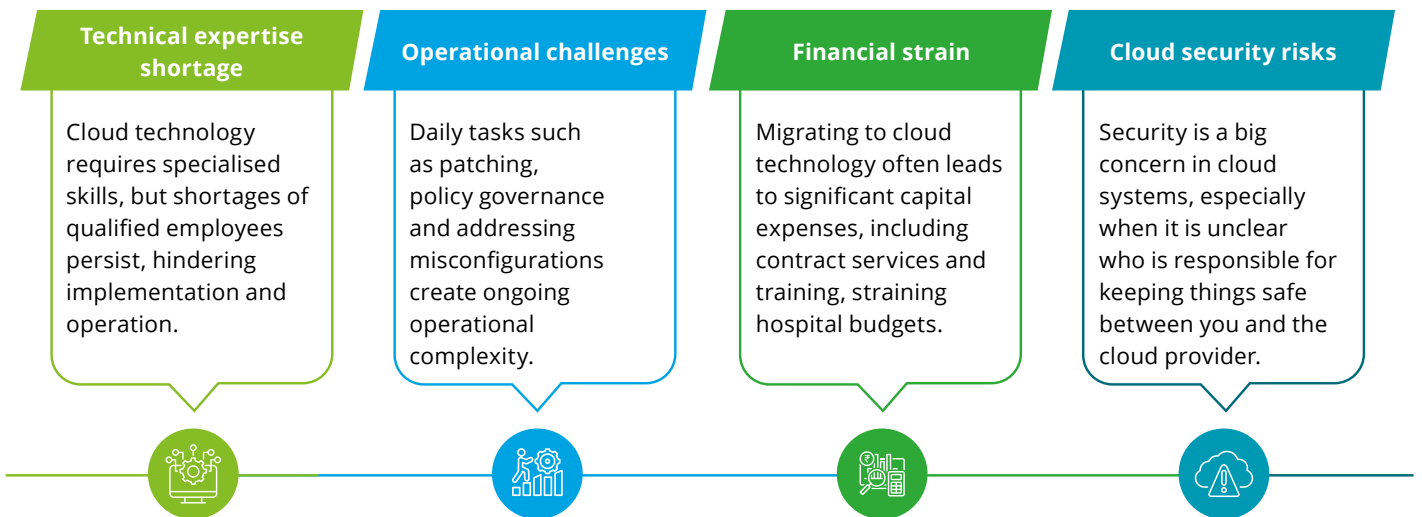


Key areas of digitalisation



Healthcare's digital shift through cloud migration in hospitals

Cloud technology is transforming healthcare by facilitating efficient analysis of patient data through hybrid cloud computing. Hospitals use this innovation through a private cloud-computing system, simplifying patient treatment nationwide. Here are a few challenges observed from the adoption of cloud technology in hospitals:



Insights from a survey on hospital cloud migration strategies⁵

Per our discussion with industry experts, who are largely CIOs of leading hospitals in India, on average, hospitals have less than 20 percent of their workloads on the cloud, except for a few specialist hospitals with more than 50 percent.

Before proceeding with migration, stakeholders need to carefully evaluate the cloud risks, whether technical,

cybersecurity or regulatory. They should recognise the importance of thorough risk assessment to ensure the security and compliance of their cloud environments.

Most hospitals believe in a structured and planned adoption of the cloud. They understand the benefits of cloud technology but emphasise the importance of strategic planning and implementation to mitigate potential challenges and risks.


⁵ Crisis Resolution & home Treatment, NIMH (E) in conjunction with the Centre for Community Mental Health, UCE Birmingham; https://bcuassets.blob.core.windows.net/docs/ccmh_crrht_full_report.pdf


Exploring the dynamic landscape of healthcare: The hospital ecosystem in India


India's hospital ecosystem is currently a diverse and dynamic landscape that provides healthcare services to over 1.3 billion people and beyond to foreign nationals. Hospitals represent a multifaceted and evolving landscape characterised by both public and private providers, and technological innovation and ongoing efforts will address healthcare challenges and


improve access to quality healthcare services for the entire population.


According to a recent survey,⁶ the hospital industry in India is projected to experience significant growth driven by multiple factors such as:


- 


Government initiatives⁷: Government initiatives aimed at improving healthcare infrastructure and access, such as the National Health Mission (NHM), Pradhan Mantri Matru Vandana Yojana (PMMVY), National Tuberculosis Elimination Programme (NTEP), National AIDS Control Programme (NACP), Mission Indra Dhanush and Ayushman Bharat, are likely to contribute to the growth of hospitals in India. Ayushman Bharat, now called the Pradhan Mantri Jan Arogya Yojana (PMJAY) currently has a network of 12,881 private hospitals that are empaneled⁸ but this percentage might increase.
- 

Investments: Ongoing investments by both public and private sectors in healthcare infrastructure, including the expansion of hospital chains and establishment of new healthcare facilities, could fuel growth.
- 

Technology adoption: Increasing adoption of technology in healthcare delivery, such as telemedicine, digital health solutions and Electronic Medical Records (EMR), enhances the efficiency and effectiveness of hospitals, driving growth.
- 

Health insurance coverage: The expansion of health insurance coverage, particularly through government-sponsored schemes such as Ayushman Bharat,⁹ might increase patients' preference for hospitals, leading to higher demand for services.
- 

Demographic trends: India's demographic trends, such as population growth, urbanisation and an ageing population, are likely to drive the demand for healthcare services.
- 

Disease burden: The increasing prevalence of lifestyle-related diseases, Non-Communicable Diseases (NCDs) and chronic conditions may lead to higher usage of hospital services, especially in cardiology, oncology and orthopaedics.
- 

Regulatory environment: Changes in the regulatory environment, including healthcare policies and accreditation standards, may affect the growth trajectory of hospitals by influencing investment decisions and operational practices, medical tourism, quality, and accreditation, rising disposable income and more.

⁶ The past, present, and future of health economics in India, Journal of Family Medicine and Primary Care, 17 January 2023; <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10040988/#:~:text=There%20have%20been%20several%20factors,Government's%20emphasis%20on%20improving%20healthcare>
⁷ Initiatives to Promote Indian Healthcare Industry, Ministry of Health and Family Welfare, Government of India, Press Information Bureau, 20 July 2021; <https://pib.gov.in/Pressreleaseshare.aspx?PRID=1737184>
⁸ Private hospitals pull back on Ayushman Bharat amid low state funding, LiveMint, 8 May 2024; <https://www.livemint.com/industry/private-hospitals-pull-back-on-ayushman-bharat-amid-low-state-funding-11715151502802.html>
⁹ Ibid.

Unlocking potential: The crucial role of digitisation in public healthcare

Advancements in technology and digitisation have led to a greater boon in the medical industry. Hardcopy versions of patients' therapeutic records are now replaced by digital copies, and specific therapeutic records can be easily retrieved digitally. This has enhanced public healthcare by improving efficiency, accessibility, quality of care and health outcomes.

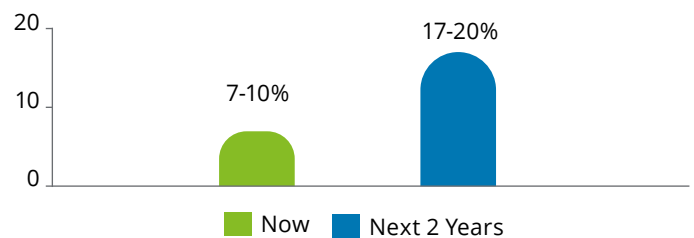
During the pandemic, most patients preferred home healthcare and telemedicine. For instance, a patient from a rural area can connect with a specialist from an urban area during an emergency due to e-consultation.

However, the percentage of preference for telemedicine and home healthcare drastically decreased post-pandemic, as patients are opting for offline consultation as their priority and optionally preferring telemedicine consultation only for follow-up consultations.

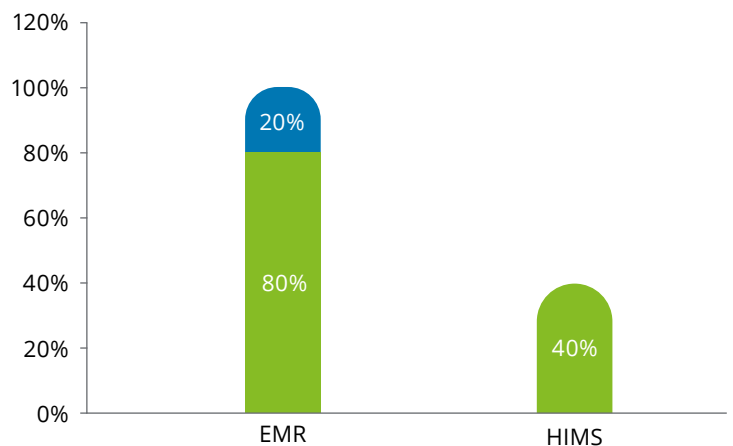
The hospital ecosystem and its growth chart display some of the digitisation contribution aspects recorded in a survey conducted on multiple private hospitals from the present to the next two years.

This study shows the current percentage of consultations coming from telemedicine and the expected increase over the next two years.

Telemedicine and remote consultation



This study illustrates the adoptability of EMRs in hospitals and their integration with other Health Management Information Systems (HMIS).
***80 percent of hospitals maintain EMRs, with 40 percent having integrated EMRs into HMIS.**



Source: DSCI-Deloitte analysis

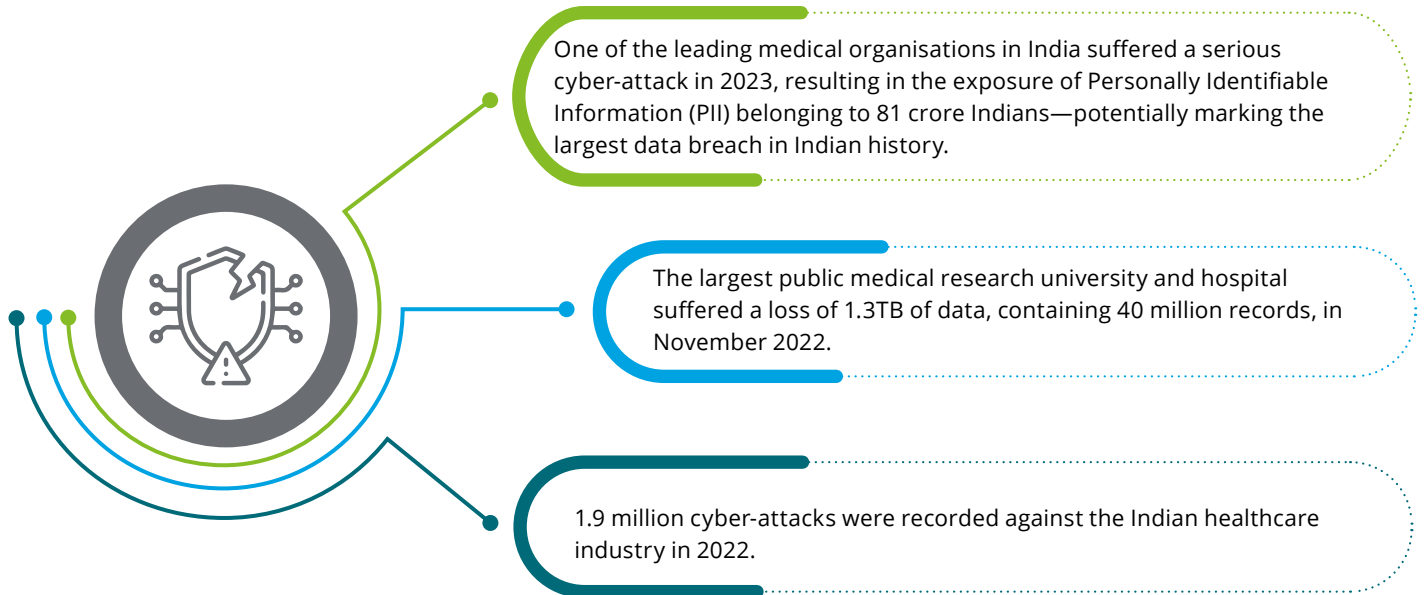


Indian hospitals' perspective: Cybersecurity challenges and solutions

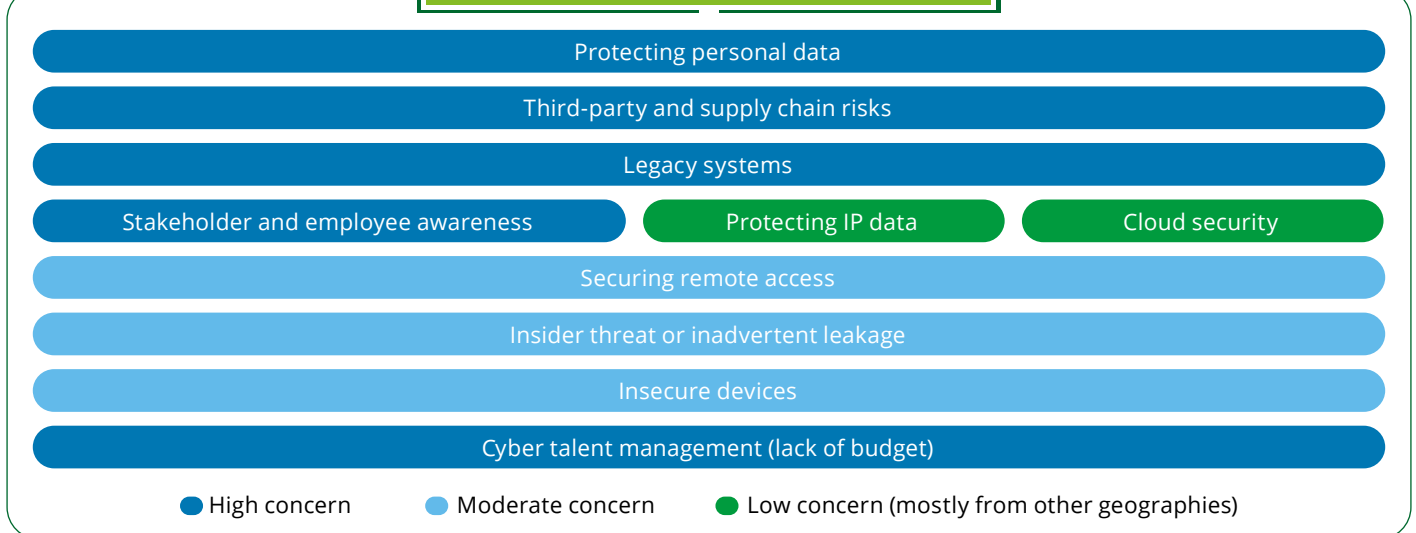
Impact of digital transformation and pandemic: Challenges, threats and vulnerabilities

While digitisation in hospitals has undoubtedly benefited both the rural and urban populations of India, it has also exposed the sector to cyber-attacks, a trend observed globally.

Recent cyber-attacks in the Life Sciences and Healthcare Industry



Key cybersecurity challenges across hospitals

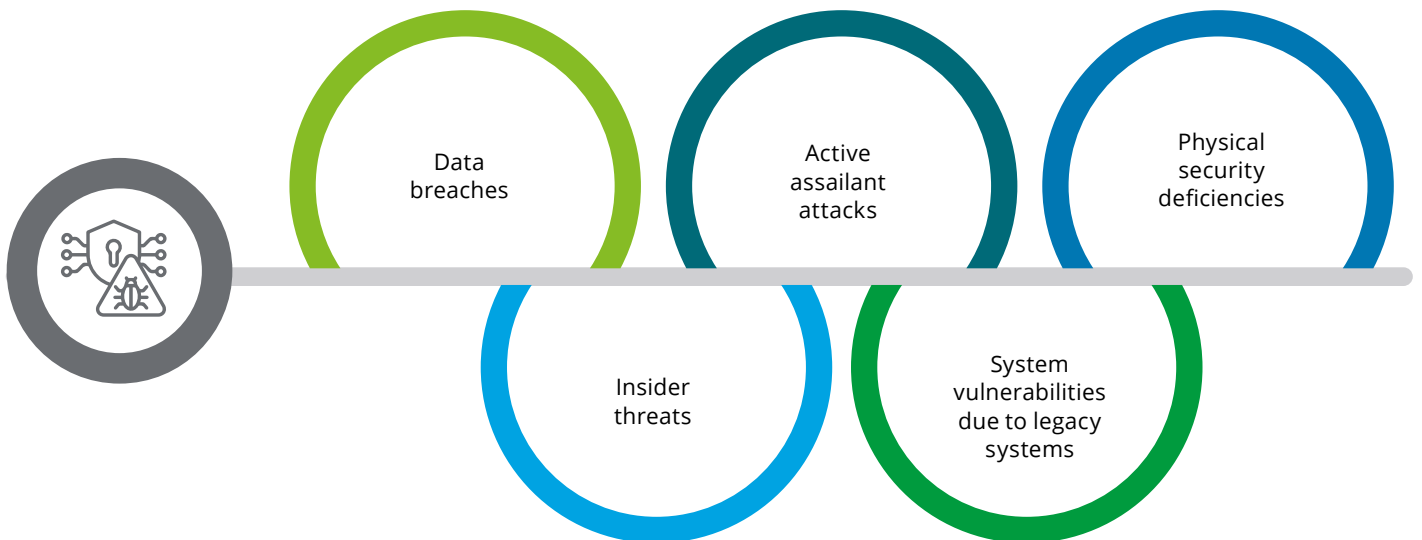




Threats and vulnerabilities¹⁰

The healthcare industry holds many sensitive information, such as medical records and other personal data. Cybersecurity threats, such as ransomware or data breaches, compromise this information and potentially result in financial harm or identity theft.

Hospitals are particularly lucrative targets for cyber attackers as they aim to access sensitive health and medical records information. The following are the top vulnerabilities:



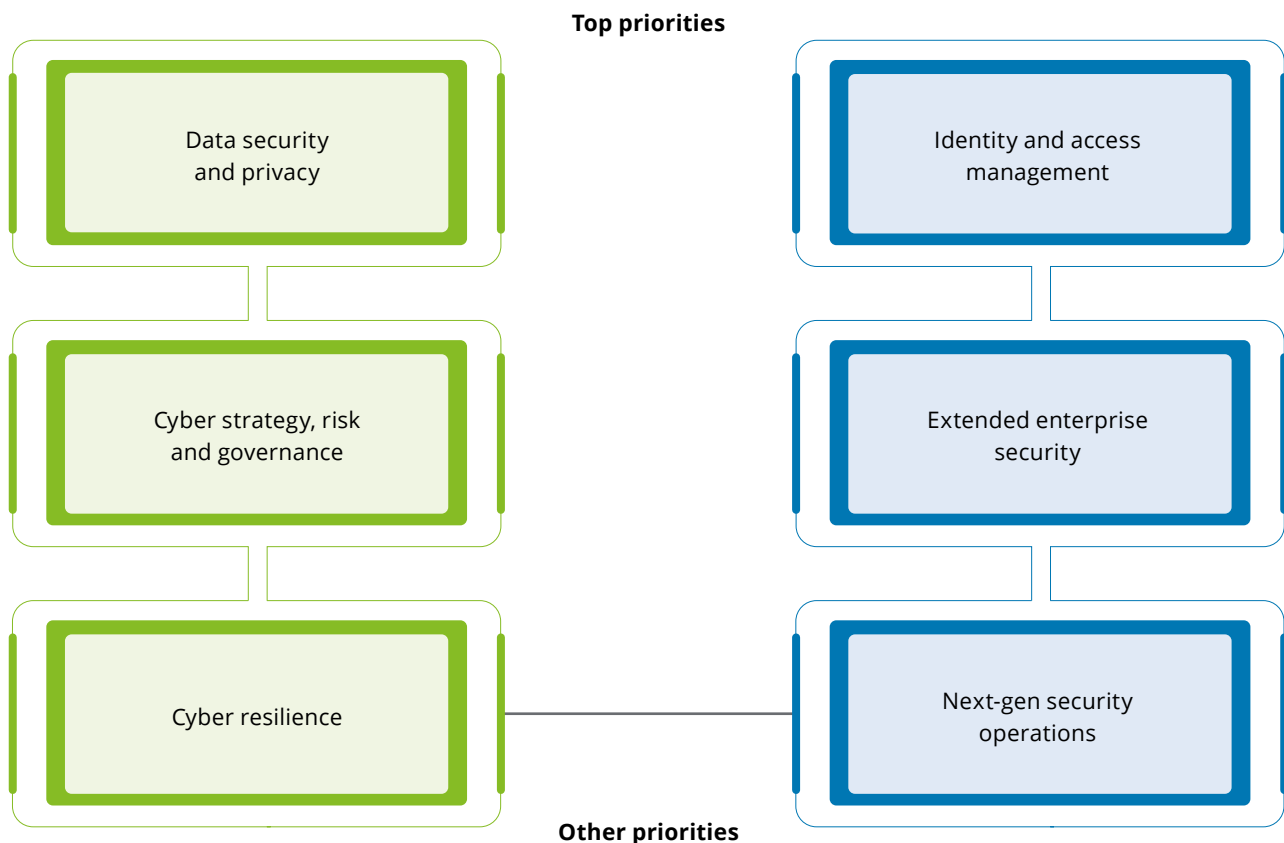
¹⁰ Cyberattacks on healthcare sector rising, 60% of organisations hit in a year: report, Economic Times, 3 November 2023; <https://economictimes.indiatimes.com/tech/technology/cyberattacks-on-healthcare-sector-rising-60-of-organisations-hit-in-a-year-report/articleshow/104917689.cms>

Security investments, priorities, and Security Operations Centre (SOC) in hospitals

On an average, hospitals spend **8-10 percent** of their IT budget on cybersecurity techniques, such as hiring professionals and acquiring tools to minimise cyber-attacks to the maximum extent.

Our survey conducted on hospitals indicates that this percentage may increase to **12-15 percent** in the next two years.

Securing tomorrow: Focus areas for the healthcare industry in the next two years



Focus areas: Infrastructure, endpoint and application security, security for emerging tech, cloud security and IoT security.

Use of SOC in hospitals

In November 2022, one of the largest hospitals in India experienced a cyber-attack in which the entire digital infrastructure collapsed due to a ransomware attack launched by external hackers. This resulted in the compromise of sensitive personal data of about 4 crore patients.¹¹

Keys issues in this case and other medical hospitals

A thorough examination was conducted on this cyber-attack, and below were the key findings:

- The IT department lacks access to the database and security despite recommendations from the National Informatics Centre (NIC).
- There was no disaster backup mechanism in place, which is essential to maintain continuity of operations.
- There were no Service Level Agreements (SLAs) between the hospital and NIC. While the hospital used to operate its own servers and security patches, no recent updates were performed.

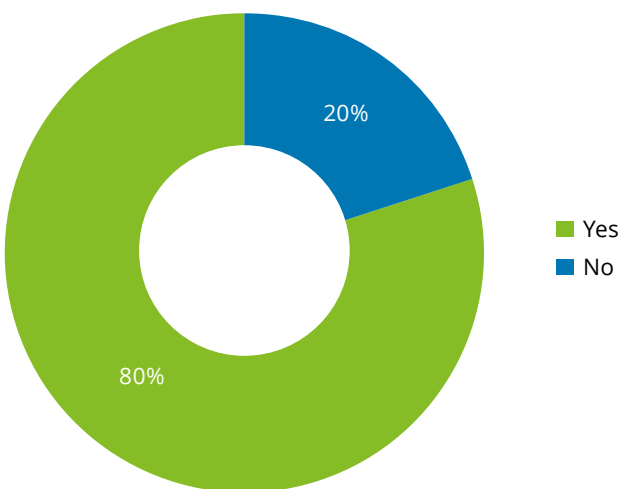
- Cyber safety and cyber resilience measures were not implemented, indicating a lack of cyberculture:
 - No NIC-recommended security audits were conducted.
 - Medical staff used personal email IDs instead of hospitals' email IDs for official activities.
 - There were no workshops and educational seminars on cyber hygiene for medical IT staff and doctors.

With the increasing frequency of cyber-attacks in Indian hospitals, there is a pressing need for a 24x7 Security Operations Centre (SOC). While private hospitals have implemented SOCs, it is essential to extend this practice to all public and private hospitals in India.

Today's scout: SOCs in hospitals

An SOC cultivates a round-the-clock security mindset to safeguard patient data and healthcare operations. Discussions and interviews with both established and emerging hospitals revealed that the majority operate an in-house SOC, while some have outsourced this service. Some have not yet implemented a SOC but have it in their pipeline or plans.

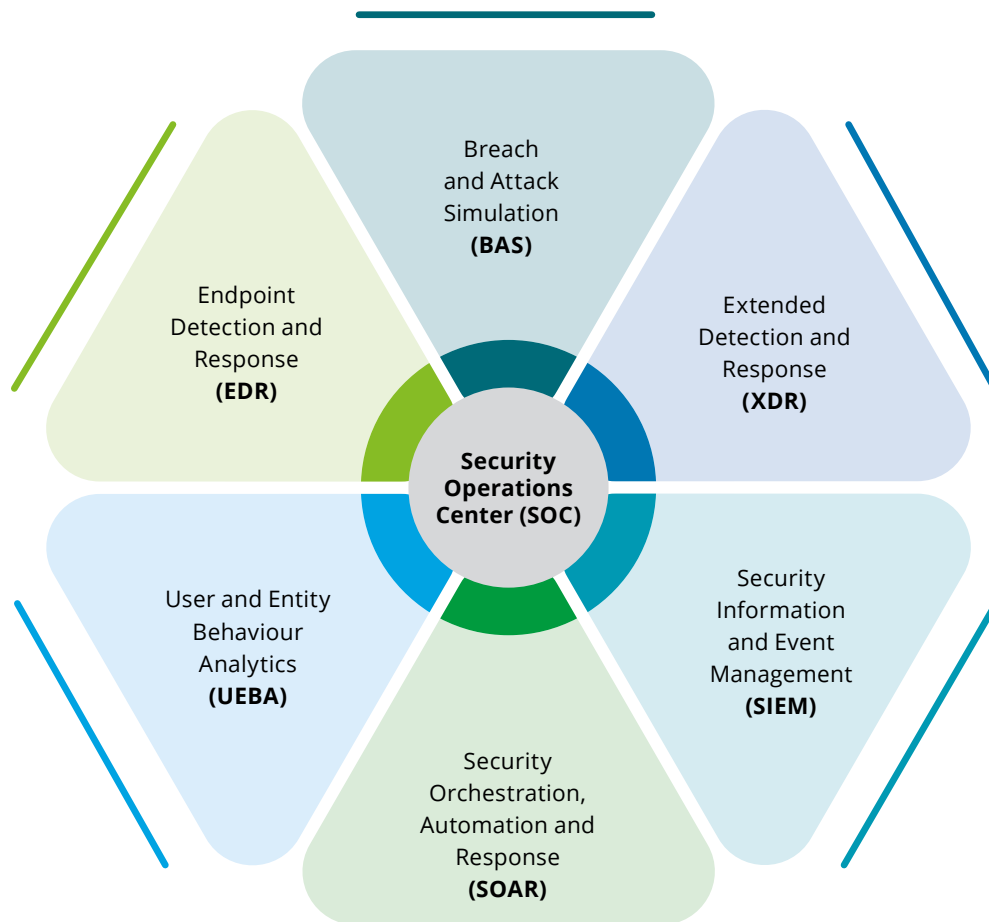
Current SOC Adaptability



This analysis demonstrates the current adaptability of SOC in hospitals. Further, hospitals that have implemented SOC operate either with an in-house, outsourced or hybrid model.

¹¹ Cyber attack at AIIMS Delhi: Hackers demand Rs 200 cr in crypto, says report, Business Today, 29 november 2022; <https://www.businesstoday.in/latest/in-focus/story/cyber-attack-at-aiims-delhi-hackers-demand-rs-200-cr-in-crypto-says-report-354475-2022-11-28>

Tools and technologies used by leading hospitals



Source: DSCI-Deloitte analysis

The crucial role of SOC

1. **Efficient operations with SIEM integration:** The SOC's pivotal role in monitoring and offering actionable guidance, based on detailed log information and real-time alerts, ensures seamless healthcare operations.
2. **Ensuring patient safety through IoT security:** The SOC's engagement in a comprehensive connected medical device and IoT security programme evaluates vulnerabilities, implements security controls and adheres to organisational standards, prioritising patient safety.
3. **Proactive defence against phishing threats:** The SOC services, including managed phishing and employee education, fortify awareness and enable proactive responses to phishing threats through well-organised simulations.
4. **Data protection through Endpoint Detection and Response (EDR):** Effective EDR within an SOC identifies and promptly addresses security threats, with a specific focus on safeguarding Protected Health Information (PHI) and PII.

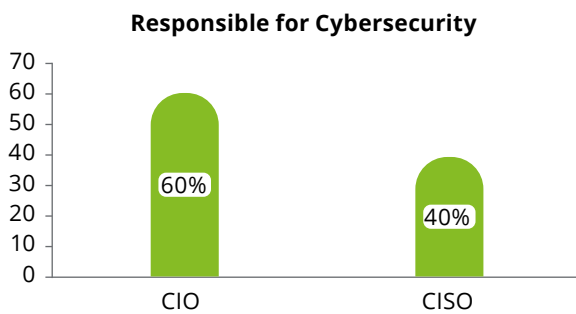
¹² SOC in Healthcare: Detecting and Responding to Security Threats, Skillmine; <https://skill-mine.com/soc-in-healthcare-detecting-and-responding-to-security-threats/>

Security and privacy governance in hospitals

In 2017-2018, as digitisation became more ubiquitous, cybersecurity started gaining prominence. Security as a function began branching out from traditional IT, but it was the pandemic that transformed the way hospitals view cybersecurity.

A Cybersecurity governance

In large hospitals, CISOs and CIOs are primarily responsible for managing cybersecurity.



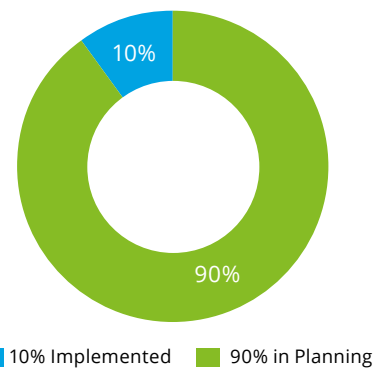
Source: DSCI- Deloitte Analysis

B. Privacy governance

The maximum percentage of hospitals indicates that data privacy is still very niche, highlighting the need for a privacy roadmap.

Only 10 percent of hospitals have fully implemented data privacy programmes, with most still in the planning stage. However, this number could increase with the introduction of the **Digital Personal Data Protection Act (DPDPA)**.

Implementation of Privacy Programs



Source: DSCI- Deloitte Analysis

Medical and cyber relations¹³

In today's internet-driven world, digitisation has been a game-changer, offering users the convenience of one-click access right at their fingertips. However, on the other end, it has led to a rise in cyber threats. Black hats (hackers) are continuously seeking

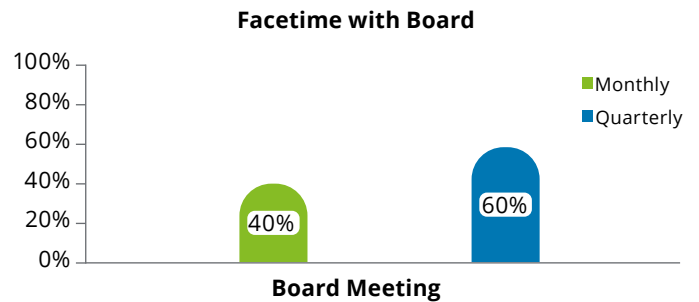
new tactics to exploit technology for malicious and unethical activities, including social engineering attacks, phishing attacks, impersonation, clickjacking and more. A cyber breach survey conducted across multiple hospitals found that most attacks happen due to a lack of cyber awareness, phishing, cloud vulnerabilities, insider threats and more.



¹³ Cyberattacks on the Healthcare Sector, Check Point; <https://www.checkpoint.com/cyber-hub/cyber-security/what-is-healthcare-cyber-security/cyberattacks-on-the-healthcare-sector/>

Strategic cybersecurity: Board and management involvement in cyberspace

With the rise in targeted attacks on hospitals, the board and management must actively engage in **cyber strategy and governance**. This includes staying updated on the latest developments, engaging in risk discussions, participating in crisis simulation activities and reviewing resilience plans. Notably, management meetings occurred monthly in all hospitals, during which Deloitte and DSCI interacted regularly.



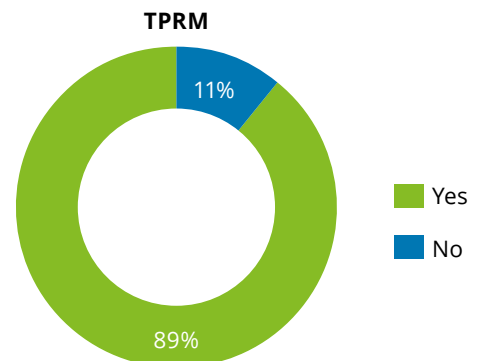
Source: DSCI- Deloitte Analysis

Board's integral role in hospital cybersecurity

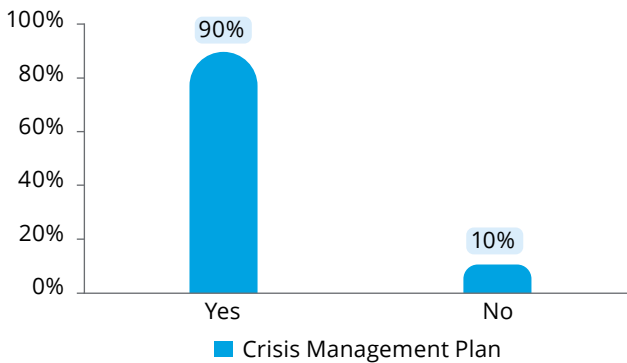
- 01 **System visibility oversight:** Implement vigilant monitoring of key clinical and financial systems to enhance visibility and promptly detect any anomalies or suspicious activities.
- 02 **Strategic cyber resilience review:** Conduct an in-depth review of cyber strategy and resilience plans to strengthen preparedness against cyber threats and ensure the ability to effectively respond and recover from incidents.
- 03 **Addressing patient-centric cyber concerns:** Prioritise cybersecurity concerns related to patient experiences to ensure comprehensive protection of sensitive medical data and maintain patient trust and confidence in the healthcare system.
- 04 **Fostering a cybersecurity culture:** Actively promote cybersecurity as an integral part of the organisational culture, encouraging all staff members to be vigilant and proactive in identifying and mitigating cyber risks.
- 05 **Active participation in exercises:** Encourage active involvement in cyber tabletop exercises to simulate real-world cyber incidents and enhance the organisation's readiness to respond effectively in an actual cyber-attack.
- 06 **Strategic budget allocation:** Directly allocate the security budget to implement effective cybersecurity measures aligned with the organisation's risk profile and priorities.
- 07 **Ensuring regulatory compliance:** Ensure compliance with relevant regulatory requirements for cybersecurity, including timely reporting of security incidents or breaches to regulatory authorities to avoid penalties and maintain stakeholder trust.
- 08 **Board-level cyber risk discussions:** Facilitate thorough discussions on cyber risks at the board level, even in hospitals without a dedicated risk committee. This will ensure a comprehensive understanding of the organisation's cyber risk landscape and informed decision-making regarding cybersecurity strategies and investments.

Hospitals and their key pillars of resilience

TPRM: Third Party Risk Management Research shows that 89 percent of hospitals already have TPRM, which helps healthcare institutions detect and address cybersecurity threats in their vendor network, protecting patient data and improving vendor relationships.



Source: DSCI-Deloitte Analysis

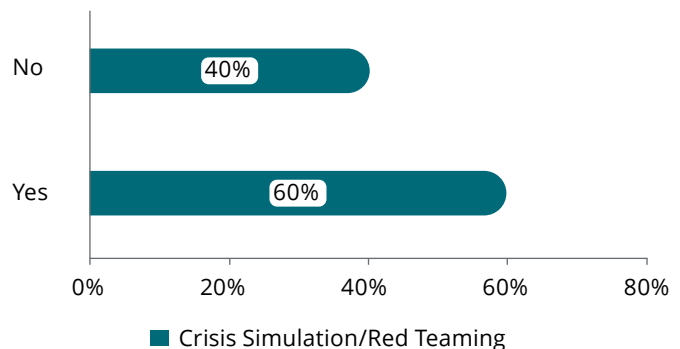


Source: DSCI-Deloitte Analysis

Crisis management plan: The survey shows that 90 percent of hospitals have adopted crisis management plans. These plans assist in responding to cyber-attacks, data theft and emergencies, ensuring uninterrupted operations and optimal patient care.

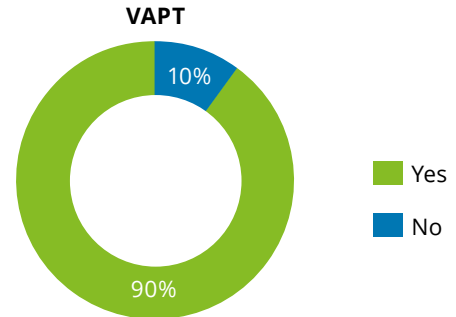


Crisis simulation/red teaming: The survey found that only 60 percent of hospitals conduct crisis simulation exercises and Red Teaming. However, 40 percent do not engage in these exercises or have them in their plans.

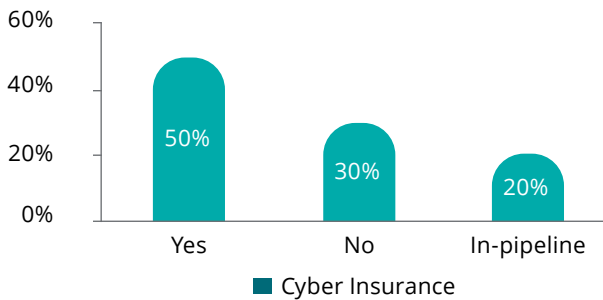


Source: DSCI-Deloitte Analysis

VAPT: 90 percent of hospitals conduct Vulnerability Assessment and Penetration Testing (VAPT) exercises annually, semi-annually or biennially.



Source: DSCI-Deloitte Analysis

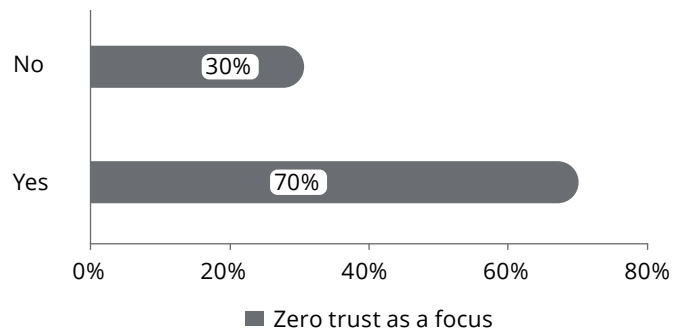


Source: DSCI-Deloitte Analysis

Cyber insurance: 50 percent of hospitals have implemented cyber insurance to mitigate the costs of data breaches. This coverage includes fines and fees resulting from ransomware attacks and phishing incidents.



Zero trust as a focus: 70 percent of hospitals prioritise Zero Trust as a crucial security initiative.



Source: DSCI-Deloitte Analysis

Benchmarks: Some hospitals adhere to the ISO 27001 and NIST Framework, while others lack a defined standard due to being in the planning stage or facing uncertainty surrounding the decision.





Way ahead and conclusion

Key takeaways

Progress in the healthcare industry: India's healthcare industry has made significant strides in specialised fields, such as cardiology and orthopaedics within private hospitals.

Digital technology acceleration: The COVID-19 pandemic has expedited the adoption of digital technologies in healthcare, leading to more cost-effective and superior therapeutic interventions.

Investment in technological advancements: Leading hospitals invest in various technological advancements, such as diagnostics, remote monitoring, AI-enabled diagnosis and IoT devices. They also explore concepts such as "hospitals without walls" and vertical integrations.

Government initiatives and regulatory environment: Government initiatives, investments and favourable regulatory environments, coupled with increasing health insurance coverage and demographic trends, are driving growth in the healthcare sector.

Digitisation's impact on public healthcare: Digitisation has notably enhanced efficiency, accessibility and health outcomes in public healthcare settings.

Challenges faced: Despite progress, challenges such as shortages in technical expertise, operational complexity, financial strain and cybersecurity risks persist.

Cybersecurity imperatives: Hospitals prioritise cybersecurity initiatives, including TPRM, crisis management plans, vulnerability assessments, penetration testing and cyber insurance.

Investment in cybersecurity: Hospitals are increasing cybersecurity investments due to rising cloud workloads and an expected surge in teleconsultations. They are focusing on data security, privacy, resilience, strategy and TPRM.

Board Involvement in cybersecurity: Cybersecurity initiatives are gaining traction at board levels, with discussions involving technology leaders in monthly or quarterly meetings.

Future outlook: The healthcare sector is poised for increased investment in cybersecurity across people, processes and technologies. Proactive measures for cyber threat hunting and defence will ensure uninterrupted healthcare services, maintaining the focus on delivering world-class healthcare to patients and communities.

Conclusion

As cloud capabilities continue to escalate annually and a 50 percent surge in teleconsultations is projected over the next 5–10 years, the need for heightened cybersecurity measures within hospitals becomes increasingly evident. Key priorities include fortifying data security and privacy, bolstering cyber resilience, refining cyber strategy and enhancing TPRM protocols.

Nearly 80 percent of hospitals have invested in foundational cybersecurity architecture, notably establishing Security Operations Centers (SOCs). The momentum behind cybersecurity initiatives is further propelled by board-level

engagement, with discussions revolving around cyber strategies frequently involving technology leaders in monthly or quarterly board meetings.

In summary, there is a clear trajectory towards amplified investment in cybersecurity across the healthcare sector's spectrum of people, processes and technologies. This entails proactive measures for both cyber defence and the pursuit of cyber threat-hunting mandates. By prioritising cybersecurity, hospitals safeguard against disruptions and uphold their core mission of delivering world-class healthcare services to patients and communities.

Connect with us

Deloitte India

Sathish Gopalaiah

President, DSA T&T
sathishtg@deloitte.com

Deepa Seshadri

Partner & Leader - Cyber,
Deloitte South Asia
deseshadri@deloitte.com

Gaurav Shukla

Partner, Deloitte India
shuklagaurav@deloitte.com

Joydeep Ghosh

Partner, Deloitte India
joghosh@deloitte.com

Antony Prashant

Partner, Deloitte India
prantony@deloitte.com

Sowmya Vedarth

Partner, Deloitte India
sovedarth@deloitte.com

Dr. Vikram Venkateswaran

Partner, Deloitte India
vikramv@deloitte.com

Data Security Council of India

Vinayak Godse

CEO, DSCI
ceo@dsci.in

Atul Kumar

Lead – Government Initiatives and Global Trade
DSCI
atul.kumar@dsci.in

Contributors

Deloitte India

Manishree Bhattacharya
Rajat Kothari
Manan Chaturvedi
Sunita Kumari
Leekshika M

Data Security Council of India

Ankit Bhadola
Amit Kr. Ghosh
Charu Sharma

About

Deloitte Touche Tohmatsu India LLP

Deloitte is one of the world's largest and most diversified professional services organisations, providing assurance and advisory, tax, management consulting, and enterprise risk management services through more than 345,374 professionals in more than 150 countries. Our organisation includes a unique portfolio of competencies integrated in one industry-leading organisation. Deloitte Touche Tohmatsu India LLP (DTTI LLP) is a member firm in India that provides non-audit consulting services. Our experienced professionals deliver seamless, consistent services wherever our clients operate. In India, Deloitte is spread across 12 cities with over 12,000 professionals, who are proficient at delivering the right combination of local insight and international expertise to our clientele drawn from across industry segments.

Deloitte is well-equipped to deliver solutions to the complex challenges faced by organisations across the public and private sectors. Our edge lies in our ability to draw upon a well-equipped global network and teaming this with customised services at a local office. We have been consistently recognised as leaders by Gartner in the Data and Analytics space, as well for Public Cloud Infrastructure Managed and Professional Services and Oracle Clod Application Services.

<https://www2.deloitte.com/in/en.html>

Data Security Council of India (DSCI)

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, setup by Nasscom, committed towards making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, CII, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

<https://www.dsci.in/>



Copyright ©2024

The information contained in this report has been obtained or derived from sources believed by DSCI to be reliable. However, DSCI disclaims all warranties as to the accuracy, completeness or adequacy of such information. We shall bear no liability for errors, omissions or inadequacies in the information contained herein, or for interpretations thereof. The material in this publication is copyrighted. You may not distribute, modify, transmit, reuse or use the contents of the report for public or commercial purposes, including the text, images, presentations, etc. without prior consent from DSCI.

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of DTTL, its global network of member firms or their related entities is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication.

© 2024 Deloitte Touche Tohmatsu India LLP. Member of Deloitte Touche Tohmatsu Limited