

The necessity of healthcare cybersecurity self-evaluation

Tamanna¹, Divya², Ekta³, Tanya Yadav⁴

1-4: PG Tutor, Department of Medical Surgical Nursing, Faculty of Nursing, SGT University, Gurugram, Haryana

Corresponding Author: Divya, PG Tutor, Department of Medical Surgical Nursing, Faculty of Nursing, SGT University, Gurugram, Haryana, suhagdivya3009@gmail.com

Abstract

The Indian healthcare system is a multifaceted and interconnected network comprising government agencies, healthcare associations, service providers, medical professionals, and patients. In recent years, there has been a marked increase in cybersecurity threats targeting this sector, posing significant risks to both operational integrity and patient safety. However, there is still uncertainty around the most effective strategies to manage and mitigate these threats within the healthcare environment.

This study explores the issue through a semi-structured focus group involving five participants drawn from both the Indian healthcare and cybersecurity sectors. Through qualitative analysis of the focus group discussion, four major themes were identified. First, participants emphasized the difficulty of securing the healthcare sector due to its complexity and the sensitivity of the data it handles. Second, financial constraints were highlighted as a major hurdle, limiting the ability of many organizations to invest adequately in cybersecurity measures. Third, the discussion addressed the ongoing struggle to balance the need for patient privacy with the benefits of transparency and information sharing. Finally, the role of education and regulation was identified as crucial, with participants agreeing that more targeted training and clearer policy frameworks are needed.

The findings suggest that to effectively address these challenges, the healthcare sector requires tailored cybersecurity tools and strategies. A key recommendation is the development and adoption of a sector-specific self-evaluation tool. Such a tool would enable organizations to proactively assess their cybersecurity readiness, identify vulnerabilities before they are exploited, and take preventative action. Although a significant body of research exists on cybersecurity, there remains a gap in studies focusing on proactive approaches—particularly those that emphasize early detection and prevention. This study contributes to filling that gap and highlights the importance of empowering healthcare stakeholders with practical tools and knowledge to face the growing threat of cyberattacks.

How to cite this article: Tamanna, Divya, Ekta, Yadav T., The Necessity of Healthcare Cybersecurity Self-Evaluation. *Int J Drug Deliv Technol.* 2026;16(81s): 1080-1087; DOI: 10.25258/ijddt.16.81s.137

INTRODUCTION

Healthcare is widely recognized as one of the most vulnerable sectors to cybersecurity breaches. Since the implementation of Indian Notifiable Data Breach (NDB) scheme, the healthcare industry has consistently reported the highest number of data breaches across all sectors. This trend underscores the sector's ongoing struggle with maintaining data security and protecting sensitive patient information.

Between January 2019 and December 2023, the Office of the Indian Information Commissioner (OIIC) received 942 notifications from the healthcare sector under the NDB scheme. This figure highlights the persistent threat facing healthcare organizations and does not even include breaches reported under the *My Health Records Act 2012*. In fact, in the 2017–2018 reporting period alone, there were an additional 42 data breaches specifically related to the My Health Record system, further emphasizing the system's vulnerability.

A closer look at incidents reported in the second half of 2022 reveals the nature of these breaches. Of the 164 notifications from health service providers during that period, over half—87 cases—were the result of malicious or criminal attacks. The remainder were attributed to human error or system faults. This breakdown points to the dual challenge faced by the sector: external threats from cybercriminals and internal weaknesses, such as staff mistakes or technical issues.

The frequency and nature of these breaches indicate a critical need for more robust cybersecurity practices within the healthcare sector. As technology continues to play an increasingly central role in healthcare delivery, the risks of cyber incidents grow. Addressing these threats requires not only improved technical defenses but also greater staff awareness, stronger regulatory frameworks, and a proactive approach to risk management across the entire health system.

Table 1 Notifiable healthcare data breaches in India

Notification period	Overall number of notifications	Health information notifications	%
Jan - Jun 2019	459	105	23
Jul - Dec 2019	537	117	22
Jan - Jun 2020	518	115	22
Jul - Dec 2020	539	123	23

Jan - Jun 2021	446	85	19
Jul - Dec 2021	464	83	18
Jan - Jun 2022	396	79	20
Jul - Dec 2022	497	71	14
Jan - Jun 2023	409	60	15
Jul - Dec 2023	483	104	22
Total	4748	942	20

The healthcare sector continues to lead all industries in reported data breaches in India. During the July to December 2023 reporting period, the sector reported 104 breaches, more than double the number reported by the next most affected sector, finance, which reported 49 breaches. This ongoing trend highlights the unique vulnerability of healthcare organizations to cyber threats and the increasing sophistication of attacks targeting sensitive health data.

According to the 2020 Health Sector Snapshot, the COVID-19 pandemic significantly altered the cybersecurity landscape for Indian healthcare system. The sudden shift to remote work environments and the rapid expansion of telehealth services created new entry points for cyberattacks. These changes exposed previously unseen vulnerabilities and made healthcare an even more attractive target for cybercriminals and nation-state actors.

In response to the growing threat, the Indian Cyber Security Centre (ICSC) issued a critical alert warning of advanced persistent threats (APTs) targeting the healthcare sector. APTs involve highly sophisticated and prolonged cyberattacks, often conducted by well-resourced threat actors with the intent of stealing sensitive data or disrupting essential services. This alert emphasized the urgent need for healthcare organizations to strengthen their cybersecurity posture.

Despite mandatory reporting requirements under the Notifiable Data Breaches scheme, under-reporting remains a significant issue. The ICSC notes that many incidents go unreported, even when disclosure is required by law. This lack of transparency hinders the ability of the sector and policymakers to fully understand the scope of the threat and implement effective countermeasures.

The combination of persistent targeting, new technological vulnerabilities, and under-reporting illustrates the critical need for comprehensive, sector-specific cybersecurity strategies. Ensuring the resilience of Indian healthcare system will depend on proactive security measures, greater awareness, and adherence to reporting protocols.

India's National Digital Health Strategy emphasizes that both healthcare consumers and providers are eager to embrace digital health services—provided that their personal health information remains confidential and secure. This growing demand for digital access underscores the importance of robust cybersecurity measures that can protect sensitive data while supporting technological advancements in healthcare.

Significant research has been conducted into developing security models for the healthcare sector, particularly in the areas of electronic health records (EHRs) and blockchain technologies. These studies have explored ways to enhance data integrity, privacy, and secure access. However, there remains a critical gap in understanding the healthcare sector's capacity to evaluate its own cybersecurity readiness. In other words, while technology solutions exist, there has been limited focus on whether healthcare organizations can proactively assess and improve their cybersecurity capabilities.

Proactive cybersecurity refers to the actions and strategies implemented before a cyber threat occurs. This approach includes deploying security protocols, continuously monitoring systems, and educating staff and stakeholders to recognize and respond to potential risks. The goal is to prevent attacks before they happen by identifying vulnerabilities and addressing them in advance. This differs from reactive cybersecurity, which involves responding to incidents only after they have already occurred, such as patching a breach or recovering compromised data.

By adopting a proactive stance, the healthcare sector can significantly reduce the impact of cyber threats. However, for this to be effective, organizations need tools and frameworks that allow them to assess their current cybersecurity posture and make informed improvements. Without the ability to self-evaluate and prepare in advance, the sector remains at risk of ongoing disruptions, data breaches, and loss of public trust. Strengthening proactive cybersecurity practices is therefore essential for ensuring a resilient and secure digital health environment in India.

Implementing proactive cybersecurity measures provides individuals, organizations, and entire sectors—such as healthcare—with a greater sense of empowerment. Empowerment, in this context, refers to the process by which individuals gain control, confidence, and the necessary tools to influence outcomes within their environment. When applied to cybersecurity, this concept helps people and institutions feel capable of identifying, managing, and mitigating threats before they escalate into serious incidents.

The concept of empowerment was first theorized by Rappaport, who emphasized its importance in enabling individuals to gain mastery over their own lives and environments. In essence, empowerment boosts a person's or group's belief in their ability to succeed. In the field of cybersecurity, this means equipping stakeholders—whether healthcare professionals, administrative staff, or patients—with the knowledge and tools necessary to understand

risks and take informed action to reduce them. It is no longer enough for cybersecurity to be the sole responsibility of IT departments or specialists. Instead, security needs to be a shared responsibility, with individuals playing a central role.

Proactive cybersecurity emphasizes prevention over response. This approach includes installing protective systems, conducting routine monitoring, developing clear policies, and most importantly, educating users on potential threats such as phishing, ransomware, and social engineering. When individuals are trained and aware of the role they play in cybersecurity, they are better positioned to contribute to a safer digital environment. They can identify suspicious behavior, report incidents early, and follow best practices that reduce the likelihood of a successful attack.

Although cybersecurity specialists are crucial for designing and managing the overall security infrastructure, their efforts are significantly enhanced when individuals within the organization actively participate in security practices. Empowered individuals are more likely to take ownership of cybersecurity responsibilities and contribute positively to the organization's resilience. In the healthcare sector—where patient data is highly sensitive and systems are critical to human wellbeing—this collaborative and empowered approach is especially vital. It ensures that all stakeholders are aligned in safeguarding information, maintaining trust, and supporting uninterrupted healthcare delivery.

Despite the implementation of sophisticated technical safeguards, human error and a lack of cybersecurity awareness remain major vulnerabilities within healthcare organizations. These gaps can allow cybercriminals to bypass even the most advanced systems, leading to severe and immediate consequences. Real-world examples show how a single moment of carelessness can lead to devastating outcomes for both patients and providers.

One such incident occurred in 2020 at the University of Vermont Health Network, where a cyberattack caused widespread disruption. Within minutes of the attack, the organization lost access to critical internal systems, including intranet services, clinical platforms such as laboratory, pathology, pharmacy, and radiology systems, as well as email communication tools and electronic medical records. These systems remained offline for nearly a month, yet the healthcare provider was still required to deliver essential patient services during the downtime. The cause of the breach was traced back to an employee who had opened a personal email on a hospital-issued laptop. The email, which originated from a legitimate local business that had itself been hacked, contained malware that infiltrated the network. This case clearly illustrates how non-targeted, relatively simple cyberattacks can have catastrophic effects when security protocols are not followed or understood.

A more recent incident in India further underscores the dangers of compromised credentials and poor cyber hygiene. In 2022, health insurer Medibank Private reported detecting “unusual activity” on its network. On December 1st, Medibank confirmed that highly sensitive data belonging to 9.7 million current and former customers had been released on the dark web. This data included personal details and healthcare claim information, raising serious privacy and safety concerns. Reports indicated that the breach was likely the result of stolen credentials from a high-ranking Medibank employee. While the company has not officially disclosed how these credentials were obtained, the attack appears to have required minimal technical sophistication. Criminals were able to exploit access to legitimate login information to infiltrate the system.

Both of these cases highlight a critical issue in modern cybersecurity: the human element. Neither the University of Vermont Health Network nor Medibank Private fell victim to highly complex or novel cyberattacks. Instead, the breaches were made possible by common security lapses—clicking a malicious link or failing to protect access credentials. These incidents reinforce the importance of comprehensive cybersecurity education and regular training for all staff members, regardless of their role.

In healthcare, where digital systems manage sensitive data and are essential to patient care, the stakes are incredibly high. Even short-term disruptions can delay treatments, compromise patient safety, and erode public trust. Thus, it is not enough to invest in technical infrastructure alone. Organizations must prioritize building a cybersecurity culture in which every individual understands their responsibility in preventing attacks.

Ultimately, improving cybersecurity in the healthcare sector requires a dual approach: implementing strong technical defenses and cultivating awareness, vigilance, and accountability among all users. When these elements work together, healthcare organizations are better equipped to detect, prevent, and respond to the growing range of cyber threats they face.

This highlights the urgent need for a strong cybersecurity culture that extends beyond purely technical solutions. To effectively protect the healthcare sector, it is essential to understand how cultural, structural, and technological factors influence the implementation and success of cybersecurity initiatives. A one-size-fits-all approach does not work in a sector as complex and sensitive as healthcare. Protective strategies must be designed with these unique challenges in mind to ensure they are practical, relevant, and sustainable.

Empowering individuals within healthcare organizations involves more than just providing basic awareness training. While awareness is a foundational element, it must be accompanied by tailored education, role-specific guidance, and active engagement with cybersecurity practices. The reality is that many cybersecurity solutions are developed with broad industry applications in mind and often fail to address the specific needs and vulnerabilities of the healthcare environment.

Healthcare systems are particularly difficult to secure due to their interconnected infrastructure, reliance on legacy systems, 24/7 operational demands, and the handling of highly sensitive patient data. Medical staff must frequently access critical information quickly, which can make strict security controls seem burdensome or counterproductive in fast-paced clinical settings. Additionally, the diversity of roles—from clinicians and administrators to third-party vendors—creates a wide range of potential access points that cybercriminals can exploit.

Therefore, developing a robust cybersecurity culture in healthcare must involve sector-specific tools, policies, and training programs that reflect the realities of healthcare work. Encouraging shared responsibility, integrating security into daily workflows, and supporting proactive engagement are all essential steps. By aligning cybersecurity strategies with the unique operational and human factors of the healthcare sector, organizations can build resilience, reduce vulnerabilities, and better safeguard both patient safety and sensitive information.

According to Thompson, the growing reliance on information technology and the vast amounts of data being collected in healthcare are placing unprecedented pressure on the sector. Traditionally, cybersecurity has not been viewed as a core responsibility within healthcare, which has led to significant challenges as digital systems become more deeply integrated into healthcare delivery.

Healthcare cybersecurity professionals often face numerous obstacles, including outdated legacy systems that are difficult to secure, limited funding for security upgrades, and a shortage of skilled cybersecurity staff. These challenges are compounded by the actions of healthcare workers who may, intentionally or unintentionally, bypass security protocols to maintain efficiency in their daily tasks. For example, workarounds—such as sharing login credentials or disabling security features—are often used to overcome the perceived inconvenience of security measures.

This situation highlights a critical gap in the sector's preparedness to handle cyber threats. As digital health continues to expand, there is an urgent need for healthcare organizations to not only invest in modern security technologies but also integrate cybersecurity as a fundamental part of healthcare operations and culture. Without this shift, the sector remains vulnerable to increasing cyber threats that could compromise patient safety and data privacy.

Despite the significant challenges faced by the healthcare sector, empowering individuals within the organization can help overcome these obstacles. When healthcare staff are empowered, they gain the knowledge and tools necessary to recognize and respond to cyber threats effectively. This includes the ability to identify suspicious emails, detect phishing attempts, and follow best practices for handling sensitive data securely.

Empowering individuals fosters a culture of cybersecurity awareness, where each staff member takes ownership of their role in protecting patient information and organizational systems. This sense of responsibility contributes to a collective defense against cyber threats, enhancing the effectiveness of technical security measures. While advanced cybersecurity technologies are essential, the vigilance and proactive behavior of healthcare workers can act as a vital line of defense, preventing many attacks before they can cause harm.

Ultimately, building a cybersecurity culture in healthcare requires integrating security into everyday practices and ensuring that all staff members are equipped with the knowledge to safeguard against evolving cyber risks. Empowered individuals, working together, can create a more resilient and secure healthcare environment, complementing and strengthening technical defenses.

To effectively empower the healthcare sector in addressing cybersecurity threats, it is crucial to gain a deeper understanding of the unique challenges and needs specific to this industry. While cybersecurity in healthcare is a global concern, the complexities and nuances of the Indian healthcare system require tailored strategies. Few studies in the India context have thoroughly examined the interplay of diverse factors that influence cybersecurity within this sector, particularly in light of its specific operational, technological, and cultural landscape.

The aim of this research is to bridge this gap by investigating the applicability of global cybersecurity trends and practices to the Indian healthcare context. We will begin by reviewing recent literature that identifies common vulnerabilities, challenges, and potential solutions within the global healthcare cybersecurity landscape. This global perspective will provide valuable insights into the common themes and issues faced by healthcare organizations worldwide, such as the growing reliance on digital systems, increased cyberattack risks, and the challenges of securing sensitive patient data.

Following this literature review, we will conduct a focus group involving healthcare professionals, IT specialists, and cybersecurity experts to explore how these established global trends align with the specific challenges and needs of the Indian healthcare system. This focus group will serve as a platform to discuss the practical realities of cybersecurity in Indian healthcare organizations, including existing vulnerabilities, technological limitations, staffing issues, and regulatory concerns.

By examining the intersection of global cybersecurity trends and the Indian healthcare context, this research will provide a comprehensive understanding of how international cybersecurity issues translate to the local environment. This two-pronged approach will not only highlight the unique challenges faced by Indian healthcare providers but also help identify gaps in current cybersecurity practices and policies.

The ultimate goal of this research is to develop practical strategies and tools that are specifically tailored to empower the Indian healthcare sector in its cybersecurity efforts. By focusing on both the global trends and the

local context, we aim to create a set of actionable recommendations that can help healthcare organizations build a robust cybersecurity framework. These strategies will emphasize proactive measures, such as improved staff education, the implementation of sector-specific security tools, and the development of a cybersecurity culture that engages all levels of the organization.

In conclusion, the research will provide a deeper understanding of the cybersecurity challenges faced by the Indian healthcare sector and offer practical solutions that address these issues effectively. By empowering healthcare professionals with the knowledge, tools, and strategies to mitigate cyber threats, this study aims to enhance the resilience of the Indian healthcare system, ensuring the protection of sensitive data and the continuity of critical healthcare services.

Literature survey

The healthcare sector has experienced a profound digital transformation in recent years, driven largely by the rise of the internet and the adoption of digital healthcare tools and technologies. These advancements have brought significant benefits, such as improved patient care and streamlined operations. However, they have also introduced a new set of vulnerabilities. As healthcare systems become increasingly interconnected, sensitive patient data, including medical records, financial information, and personal details, has become a prime target for cybercriminals.

The surge in cyberattacks targeting the healthcare sector presents serious risks to patient privacy, financial stability, and the overall quality of care. Data breaches can lead to the exposure of confidential information, putting patients at risk of identity theft and fraud. Additionally, such breaches can disrupt critical healthcare services, delay diagnoses, and even compromise patient safety. For instance, if medical records are inaccessible due to a cyberattack, healthcare providers may struggle to deliver timely and accurate care, potentially leading to adverse outcomes.

The financial impact of cyberattacks on healthcare organizations can be severe. Healthcare providers may face hefty fines for failing to protect patient data, along with reputational damage that undermines public trust. Furthermore, the costs of remediation—such as implementing security measures, conducting investigations, and notifying affected individuals—can place a substantial financial burden on healthcare institutions. As cyber threats continue to evolve, it is crucial for healthcare organizations to strengthen their cybersecurity practices to safeguard patient data and maintain the integrity of their services.

Numerous scholars have looked at literature that clarifies vulnerabilities, difficulties, and potential solutions related to cybersecurity in the healthcare industry. We have concentrated on literature evaluations that have been published in the last three years in order to obtain the most recent knowledge of this developing topic. Table 2 outlines the selection criteria for research articles.

Table 2 Research criteria

Data Source	Google Scholar
Time Frame	2020 to Now (April 2024)
Document Type	Journal articles
Keywords	How to cite this article: Tamanna ¹ Divya ² Ekta ³ Tanya Yadav ⁴ . The necessity of healthcare cybersecurity self-evaluation. Int J Drug Deliv Technol. 2026;16(81s):1080-1087. DOI: 10.25258/ijddt.16.81s.137. “healthcare” OR “health care” OR “health” AND “cybersecurity” OR “cyber” AND “literature review” OR “review”

Relevant literature reviews were found using Google Scholar. By concentrating on recent reviews, the analysis was able to take into account the most recent research and tackle the most important cybersecurity issues that healthcare organizations are currently experiencing. This work will help to identify current vulnerabilities and research needs in healthcare cybersecurity by synthesizing these reviews. A overview of the chosen research publications is given in Table 3.

Table 3 Overview of papers reviewed

Author(s)	Year	Title	Papers Reviewed	Date Range	Search Criteria
Vilakazi and Adebisin	2023	A systematic literature review on cybersecurity threats to healthcare data and mitigation strategies	41	2017 to March 2022	(“cyber”) AND “threat*” OR “attack*” OR “crime*”) AND (“health*”) AND (“data”) AND (“secur*”) OR “mitigate” OR “protect”)

Aldossri and Rahman	2023	A systematic literature review on cybersecurity issues in healthcare	21	2019 to 2022	(security or cybersecurity) AND healthcare AND (threats OR vulnerabilities OR challenges)
Herrera et al.	2023	Cybersecurity in health sector: a systematic review of the literature	71	2018 to 2022	“cybersecurity” “cyberattacks” “health” and “hospital”
Nifakos et al	2021	Influence of human factors on cybersecurity within healthcare organisations: A systematic review	70	2010 to 2021	Human AND (Cybersecurity AND “training” OR “Information security awareness”)
He et al.	2021	Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review	56	2011 to 2020	(covid OR healthcare) AND cybersecurity.
Sardi et al.	2020	Cyber-risk in health facilities: A systematic literature review	84	1992 to 2020	“Cyber” OR “Computer security” AND “Health” AND “Risk”

Vilakazi and Adebessin conducted a systematic literature review to investigate effective strategies for mitigating cybersecurity threats targeting healthcare data. Their research identified several critical vulnerabilities within healthcare cybersecurity systems, revealing both technological and human-related weaknesses. One of the primary challenges highlighted was the rapid rise of new digital technologies, which, while offering significant improvements in healthcare delivery, also introduced a range of new security risks. These technologies, such as electronic health records (EHRs) and telemedicine platforms, are often interconnected and can provide cybercriminals with multiple entry points into healthcare systems. Another vulnerability identified was the lack of established and comprehensive cybersecurity policies within healthcare organizations. Many healthcare providers still rely on outdated security protocols, and the absence of clear, standardized procedures makes it difficult to respond effectively to emerging threats. In addition to technological shortcomings, the review found that human factors, such as staff unawareness of cybersecurity risks, played a significant role in enabling cyberattacks. Healthcare professionals, often focused on patient care, may not be adequately trained to recognize cyber threats such as phishing emails or ransomware. This lack of awareness can lead to unintentional actions, such as opening malicious attachments or neglecting basic security protocols, that expose healthcare systems to attack. The review also highlighted the issue of inadequate investment in cybersecurity measures. Many healthcare organizations, particularly smaller practices, do not allocate sufficient funds to implement robust security systems or hire specialized cybersecurity personnel. This financial limitation often results in weak defenses against increasingly sophisticated cyberattacks.

Aldossri and Rahman conducted a similar study on cybersecurity challenges in healthcare, identifying several key areas of concern. Like Vilakazi and Adebessin, they emphasized the importance of addressing human factors, such as insufficient staff training and awareness. However, their research also underscored other critical issues, including technological vulnerabilities, data security and privacy concerns, insider threats, and the risk of external attacks. Insider threats, including negligent or malicious behavior by employees or contractors, were highlighted as a significant security risk. Additionally, external attacks, such as hacking or ransomware, continue to evolve, with cybercriminals increasingly targeting healthcare organizations due to the high value of healthcare data. Both studies stressed the importance of comprehensive staff training and awareness programs to combat these vulnerabilities. Ensuring that healthcare employees understand the risks associated with cyber threats and are equipped with the knowledge to mitigate them is crucial. Moreover, fostering a cybersecurity-conscious culture within healthcare organizations can significantly reduce the likelihood of human error leading to a breach. By educating staff on the importance of securing patient data and following best practices, healthcare providers can build a more resilient defense against cyber threats.

Aldossri and Rahman concluded that cyberattacks targeting healthcare institutions have significantly increased in recent years, and there are no indications that this trend will decrease anytime soon. The rise in cyber threats highlights the urgent need for proactive cybersecurity measures within the healthcare sector. The researchers emphasized that addressing these challenges requires a comprehensive and ongoing effort to educate both staff and patients about cybersecurity risks and best practices. One of the most effective ways to ensure strong

cybersecurity in healthcare, according to the researchers, is through continuous education. Healthcare staff must be regularly trained to recognize and respond to evolving cyber threats, such as phishing attacks, ransomware, and insider threats. By keeping employees informed and vigilant, healthcare organizations can reduce the likelihood of human error leading to security breaches. Additionally, Aldossri and Rahman noted the importance of involving patients in cybersecurity efforts. Since patients are often the recipients of sensitive health data, they should be made aware of the risks associated with their personal information and educated on how to protect it. This includes understanding the importance of secure communication channels, recognizing fraudulent practices, and practicing good password hygiene. Overall, the study underscores the need for a culture of continuous learning and engagement in healthcare cybersecurity. By focusing on education and awareness, healthcare organizations can build a more resilient defense against cyber threats, ensuring the protection of sensitive patient data and the continuity of essential healthcare services.

Sardi et al. conducted a literature review that further supports the themes raised by previous studies regarding the escalating cyber-risk in healthcare. Their analysis identified four key themes that contribute to the growing vulnerability of healthcare systems: human actions, system failures, internal process breakdowns, and external events. These findings align closely with the vulnerabilities highlighted in earlier research by Vilakazi and Adebisin and Aldossri and Rahman, emphasizing the need for proactive cybersecurity solutions in healthcare.

Human actions, particularly staff unawareness and negligence, remain one of the most significant contributors to cybersecurity breaches in healthcare. As mentioned in earlier reviews, many healthcare workers are often unaware of the risks posed by cyber threats, leading to unintentional actions such as opening phishing emails or failing to follow proper security protocols. Sardi et al. also emphasized that system failures, such as outdated infrastructure and software, increase the likelihood of successful cyberattacks. Many healthcare organizations still rely on legacy systems that lack adequate security features, making them prime targets for cybercriminals. Moreover, internal process breakdowns, such as poorly implemented security policies or weak communication channels between departments, further exacerbate the situation. These internal weaknesses can lead to delayed responses to cyber threats and prevent organizations from implementing necessary security measures promptly.

External events, such as the rise of sophisticated cybercriminal tactics or global cybersecurity trends, also play a significant role in the increasing cyber-risk in healthcare. Cyberattacks are becoming more advanced, with hackers utilizing techniques such as ransomware, advanced persistent threats, and data breaches to target healthcare systems. These external pressures compound the challenges already faced by healthcare organizations, making it essential to develop a multi-layered cybersecurity strategy that addresses both internal and external factors. While Sardi et al. reinforced the importance of addressing these vulnerabilities, they also identified two critical gaps in the existing research. First, they noted the lack of comprehensive studies on cyber-risk assessment in healthcare. Without a thorough understanding of an organization's unique vulnerabilities and strengths, it becomes challenging for healthcare providers to develop effective cybersecurity strategies. Cyber-risk assessments allow healthcare organizations to identify weak points in their systems, prioritize security measures, and allocate resources efficiently. Without such assessments, healthcare institutions may be ill-prepared to handle emerging cyber threats, leaving them exposed to potential attacks that could compromise patient safety, disrupt services, and damage their reputation.

The second gap identified by Sardi et al. was the lack of research focused on healthcare systems outside the United States. While much of the existing literature on healthcare cybersecurity primarily focuses on the US healthcare system, this narrow focus overlooks the unique challenges faced by healthcare sectors in other countries. Healthcare systems vary widely around the world, with significant differences in infrastructure, staffing, technological adoption, and regulatory frameworks. For example, in some countries, healthcare providers may rely heavily on paper-based systems or outdated technologies, making them more susceptible to cyberattacks. In contrast, more technologically advanced systems may face different risks, such as the increased exposure of sensitive data due to interconnected systems and cloud-based solutions. These disparities can substantially impact the types and severity of cyberattacks faced by healthcare institutions. What works as a mitigation strategy in one country may not be effective in another due to differences in healthcare infrastructure and technological maturity. Therefore, Sardi et al. emphasized the need for more research focused on understanding the specific cybersecurity challenges in diverse healthcare contexts. A more global perspective on healthcare cybersecurity will allow for the development of region-specific strategies and tools tailored to the unique needs of healthcare systems worldwide.

In conclusion, Sardi et al.'s review highlights the growing cyber-risk in healthcare and reinforces the importance of addressing human actions, system failures, internal process breakdowns, and external events in mitigating these risks. The identified gaps in research, particularly the lack of comprehensive cyber-risk assessments and the focus on the US healthcare system, underscore the need for a more nuanced, global approach to cybersecurity in healthcare. By addressing these gaps, healthcare organizations worldwide can better protect sensitive patient data, ensure the continuity of care, and build resilience against the evolving landscape of cyber threats.

Hu et al. conducted a literature review covering articles from 2011 to 2020, with a primary focus on examining the cybersecurity challenges healthcare systems faced during the COVID-19 pandemic. The rapid shift to remote

work during the pandemic exposed significant vulnerabilities in healthcare cybersecurity, highlighting the unpreparedness of healthcare organizations to secure this new, unfamiliar environment. These findings align with observations made by Herrera et al., who also noted that healthcare organizations struggled to adapt to the sudden surge in remote work, which became a critical point of weakness for many institutions.

The pandemic forced healthcare organizations to quickly transition to telemedicine, remote consultations, and home-based work environments to ensure the continuity of care while complying with social distancing regulations. However, many organizations lacked the necessary planning, security infrastructure, and cybersecurity measures to adequately protect the new remote work environment. As a result, healthcare systems became increasingly vulnerable to cyberattacks. The lack of business continuity plans meant that any disruption could have a significant impact on essential healthcare services, including diagnostics, treatment, and patient care. Furthermore, many healthcare staff were not adequately trained or equipped to recognize cybersecurity threats, making them more susceptible to phishing attacks, malware, and other forms of cybercrime.

Hu et al.'s review highlighted how these vulnerabilities contributed to a surge in cyberattacks during the pandemic, with healthcare institutions being specifically targeted by malicious actors. The rise in cyber threats, such as ransomware attacks, became more pronounced as the sector's digital footprint expanded rapidly without adequate security measures. These vulnerabilities were further compounded by the lack of security awareness training for healthcare staff. As the healthcare workforce transitioned to remote work, employees faced challenges in securing their devices and communication channels, increasing the likelihood of successful cyberattacks.

In building upon these findings, Nifakos et al. conducted a systematic review to identify recurring human behaviors that weakened the cybersecurity posture of healthcare organizations. One of the most significant takeaways from this review was the central role that human factors play in healthcare cybersecurity. Human actions—ranging from simple negligence to intentional malicious behavior—emerged as a recurring theme across the cybersecurity literature on healthcare. Nifakos et al. found that many security breaches in healthcare were the result of employees' failure to adhere to established security protocols. These breaches often occurred because healthcare staff were either unaware of the risks or too busy to follow proper procedures.

In many cases, healthcare workers were found to circumvent security protocols in an effort to streamline their work processes or overcome technical issues, unintentionally opening the door for cyberattacks. For instance, some staff members resorted to using personal devices for work-related activities, bypassing the security measures in place on organizational devices. This behavior, though often driven by the urgency of patient care or the lack of technical resources, posed a serious threat to the organization's cybersecurity. Additionally, the absence of proper security awareness training and ongoing education meant that staff members were ill-equipped to recognize common cyber threats, such as phishing emails or social engineering attacks.

Nifakos et al. also noted that healthcare organizations, particularly those in the midst of the COVID-19 crisis, failed to implement long-term planning and prepare for the broader cybersecurity risks associated with digital transformation. As the healthcare sector adopted more digital tools and technologies to accommodate the pandemic, many institutions neglected to strengthen their cybersecurity frameworks. This oversight left healthcare systems exposed to cyberattacks, which targeted both sensitive patient data and critical operational systems. The failure to adopt best practices in cybersecurity, particularly in the face of the rapid transition to remote work, made healthcare organizations highly susceptible to cybercrime.

Moreover, the findings of Nifakos et al. reinforced the need for healthcare institutions to invest in cybersecurity solutions that address human factors. They argued that improving human behavior is essential for the long-term resilience of healthcare cybersecurity. This could include regular training sessions to raise awareness about cyber threats, as well as fostering a culture of cybersecurity within healthcare organizations. By encouraging employees to take responsibility for protecting sensitive information, organizations could reduce the likelihood of insider threats, accidental breaches, or negligent behavior.

Furthermore, there is a significant research gap in the field of healthcare cybersecurity that warrants further investigation, specifically regarding comprehensive cyber-risk assessment methodologies and best practices that can be applied to diverse healthcare systems globally. One promising approach to addressing this gap could involve the development of a self-assessment tool tailored to the unique needs of various healthcare actors. Such a tool could consist of multiple sections, each designed to allow healthcare organizations and professionals to assess their cybersecurity posture effectively. The tool could be structured to address specific areas of concern such as data security, access control, incident response, and staff training, providing a comprehensive evaluation of an organization's cybersecurity measures and helping stakeholders pinpoint areas requiring improvement.

The development and implementation of such a tool would be particularly valuable in the context of the healthcare sector, where resources may be constrained, and cybersecurity threats are constantly evolving. By offering a framework for self-assessment, healthcare organizations can better understand their vulnerabilities and proactively take steps to mitigate cybersecurity risks. In addition, this tool could be adapted for use across various healthcare settings, from small clinics to large hospitals, and even extend to healthcare insurers and government bodies involved in the sector. This approach would ensure that cybersecurity measures are appropriate to the specific needs of each healthcare provider and could be integrated into existing processes without significant disruptions.

The purpose of this research is to bridge this gap by assessing the applicability of general cybersecurity findings from existing literature to the specific context of the Indian healthcare sector. India's healthcare system, with its unique combination of public and private providers, emphasis on digital health initiatives, national framework for health information privacy and security, and a nationwide health record system, presents distinct challenges and opportunities when it comes to cybersecurity. This context underscores the importance of developing tailored strategies that address the particular vulnerabilities faced by Indian healthcare organizations. By considering the general cybersecurity vulnerabilities identified in international literature and evaluating their relevance within the Indian setting, this research aims to offer valuable insights into how the country can strengthen its cybersecurity preparedness.

The Indian healthcare sector is undergoing a digital transformation, with increasing reliance on electronic health records, telehealth services, and other digital tools that connect healthcare providers and consumers. While these advancements have improved accessibility and efficiency, they have also introduced new risks, including the potential for data breaches and system vulnerabilities. Additionally, the sector faces challenges such as a lack of cybersecurity professionals, limited resources for investing in advanced security measures, and an overall underinvestment in cybersecurity compared to other industries.

To address these challenges, this research will facilitate a focus group discussion with stakeholders from various sectors of the Indian healthcare system, including healthcare providers, government representatives, and cybersecurity experts. This discussion will serve as a platform for exploring the general cybersecurity challenges identified in existing literature and assessing their applicability to the Indian context. By gathering perspectives from those directly involved in healthcare delivery and cybersecurity, the research will contribute to the development of a more nuanced understanding of the cybersecurity risks faced by Indian healthcare organizations. In addition, the findings from this research will be instrumental in guiding the development of cybersecurity strategies that are specifically designed to meet the needs of the Indian healthcare sector. The focus group will help identify priority areas for cybersecurity interventions, such as enhancing staff training, improving data protection protocols, and strengthening incident response capabilities. Ultimately, this research aims to equip Indian healthcare organizations with the knowledge and tools necessary to improve their cybersecurity resilience and better protect sensitive patient data from the increasing threat of cyberattacks.

By examining the unique challenges faced by the Indian healthcare system and identifying the most effective cybersecurity measures, this research will contribute to the broader global conversation about healthcare cybersecurity. The insights gained from this study can be used to inform the creation of self-assessment tools, best practices, and other resources that can be adapted and implemented in healthcare systems worldwide, enhancing global cybersecurity efforts and safeguarding the future of digital healthcare.

Method

This study utilized a semi-structured focus group discussion to gain in-depth insights into the current state of cybersecurity in the Indian healthcare sector. While large-scale surveys can provide a broader overview of issues, focus groups offer distinct advantages in exploring complex topics. As Crone notes, semi-structured focus groups use open-ended questions that not only elicit valuable information but also allow participants to share personal experiences, which may not have been previously considered in research. This method is particularly useful in the context of Indian healthcare, where the intersection of cultural, structural, and technological factors influencing cybersecurity has not been thoroughly examined.

The focus group was composed of a small group of key stakeholders from various sectors, including government, healthcare providers, and cybersecurity experts, creating a platform for rich discussions on the unique challenges and opportunities that the Indian healthcare system faces. According to Krueger and Casey, the focused nature of a small group allows for a deeper, more nuanced understanding of participants' perspectives and experiences. Additionally, the interaction between participants in a focus group, a key feature of this method, fosters the generation of insights that might not be accessible through individual interviews. This group dynamic facilitated a comprehensive exploration of participants' views on healthcare cybersecurity, enabling them to build on each other's ideas and perspectives.

The focus group approach also offered an opportunity for participants to engage with different viewpoints on the subject. As participants shared their thoughts, the discussion naturally highlighted areas of agreement, disagreement, and uncertainty, helping to illuminate not just the "what" of cybersecurity challenges but also the "why" and "how." This methodology ensures that the study captured a diverse range of opinions without pressuring participants toward a single, unified consensus.

While the information gathered from the focus group represents only the perspectives of those who participated, and thus cannot be generalized to the entire healthcare sector, it still offers valuable insights. The group dynamic encouraged the exchange of knowledge and experiences on the sensitive issue of healthcare cybersecurity, shedding light on both the challenges and potential solutions faced by the sector. By engaging with the existing literature alongside these participant perspectives, the study contributed to a richer understanding of the current state of cybersecurity within Australian healthcare and provided insights into the direction needed to strengthen cyber defenses.

This approach is critical in the Indian context, where cybersecurity in healthcare is an emerging but increasingly important issue. With rapid technological advancements and digital transformations in healthcare services, understanding the interplay between technology, culture, and organizational structure is vital to developing more effective cybersecurity strategies. The semi-structured focus group facilitated a space for exploring these complex factors in depth, offering valuable contributions to the ongoing conversation about cybersecurity in the healthcare sector.

Participants

To ensure diverse and comprehensive perspectives, participants were carefully recruited based on their involvement in one or more of the following areas: the Australian healthcare industry, cybersecurity practice, or cybersecurity research. Twelve organizations with ties to the Australian healthcare sector were contacted via email invitations, and five participants responded, agreeing to take part in the focus group discussion. The discussion was led by two of the authors, who were responsible for facilitating the session and ensuring that all viewpoints were heard and considered.

The participants in the focus group represented a variety of backgrounds and professional experiences. While each individual brought a unique perspective, the common thread among them was a specialized interest in the intersection of computer security and healthcare. This purposeful selection strategy was instrumental in ensuring that the group possessed both practical knowledge of the healthcare sector and a deep understanding of the complexities involved in securing digital health infrastructures. The participants' expertise in both healthcare and cybersecurity allowed for a well-rounded discussion, addressing the multi-faceted nature of the challenges at hand. The size of the focus group was deliberately kept small to foster an environment conducive to open and honest discussion. Given that healthcare cybersecurity can be a sensitive topic, it was essential to create a space where participants felt comfortable sharing their personal experiences, challenges, and insights. As a result, the group dynamics allowed for a more intimate and candid exchange of ideas, leading to a richer and more nuanced understanding of the issues and potential solutions. A smaller group setting facilitated in-depth conversations, ensuring that every participant had the opportunity to contribute meaningfully to the discussion. This approach also allowed for the exploration of issues that might not have emerged in larger group settings or through surveys. The participants in the focus group had a deep and comprehensive understanding of the Australian healthcare environment and its associated security landscape, making them well-suited to contribute to the research. Each participant's professional background added a layer of expertise that enriched the conversation. To ensure confidentiality and protect the identities of the participants, pseudonyms were assigned to each individual.

Participant 1: A Chief Information Officer (CIO) for a public regional healthcare service in Australia, Participant 1 brought invaluable firsthand experience in managing cybersecurity within a large healthcare organization. This individual had direct responsibility for overseeing the security infrastructure and was intimately familiar with the challenges of balancing patient care with the need for robust cybersecurity measures.

Participant 2: A general practitioner (GP) based in Victoria and a member of the Royal Australasian College of General Practitioners (RACGP) Expert Committee on Practice Technology and Management, Participant 2 provided a practitioner's perspective on the daily challenges of integrating technology into clinical settings. Their input was especially valuable in understanding the impact of cybersecurity policies and practices on healthcare professionals who are not cybersecurity specialists but rely heavily on secure digital tools for patient care.

Participants 3 and 4: Both were senior university researchers with extensive experience in the healthcare sector, particularly in leading research projects that focused on health technology and digital transformation. These participants brought an academic and research-based perspective to the discussion, which helped to identify evidence-based approaches and potential areas for further study. Their expertise in healthcare-specific projects added a critical layer of insight into the systemic challenges and opportunities for improving cybersecurity in the Australian healthcare context.

Participant 5: With experience at an industry-university cybersecurity research center, Participant 5 provided deep expertise in security best practices. This participant's background in cybersecurity research allowed them to bring technical insights into the discussion, offering knowledge on cutting-edge solutions, tools, and methodologies for addressing cybersecurity threats in healthcare settings. Their contribution was instrumental in discussing the feasibility of implementing advanced cybersecurity measures in healthcare organizations, considering the sector's unique limitations and needs.

The focus group discussion began with a general overview of the current state of cybersecurity in Australian healthcare, with each participant sharing their insights and experiences. Throughout the session, participants were encouraged to discuss both the technical and non-technical aspects of cybersecurity, recognizing that healthcare security involves not only the adoption of advanced technology but also the culture, structure, and behaviors within healthcare organizations.

The group delved into topics such as the lack of specialized cybersecurity staff within healthcare organizations, the challenges of maintaining outdated IT infrastructure, and the impact of insufficient cybersecurity training for healthcare professionals. Participants also addressed the broader organizational issues that contribute to

vulnerabilities, such as budget constraints and the fragmented nature of healthcare governance in Australia, which complicates the implementation of standardized security measures across the sector.

One of the key themes that emerged during the discussion was the growing need for more comprehensive cybersecurity education and awareness across all levels of healthcare organizations. The focus group emphasized that, while technological solutions are critical, human factors such as staff awareness and training play a pivotal role in preventing cyberattacks. Participants agreed that fostering a culture of cybersecurity within healthcare organizations—where staff are empowered with the knowledge and tools to recognize and mitigate threats—is essential for improving the sector's overall cybersecurity posture.

Furthermore, the group discussed the need for tailored cybersecurity strategies that account for the unique challenges faced by healthcare providers in Australia. Given the diversity of healthcare settings, ranging from small rural clinics to large metropolitan hospitals, a one-size-fits-all approach is unlikely to be effective. Participants noted that customized security solutions, informed by the specific needs and vulnerabilities of each healthcare provider, are necessary to ensure a more resilient healthcare system.

The insights gained from this focus group discussion provide valuable information for the ongoing development of cybersecurity strategies within the Australian healthcare sector. The participants' expertise and perspectives helped to identify both current vulnerabilities and potential solutions, and their suggestions will be instrumental in informing future research and policy development aimed at improving cybersecurity resilience in healthcare. This study highlights the importance of involving a diverse range of stakeholders in discussions about healthcare cybersecurity to ensure that all relevant perspectives are considered when developing and implementing security measures.

Procedure

The focus group was conducted using both face-to-face and teleconferencing methods to ensure participants could easily engage regardless of their physical location. This hybrid approach allowed for broader participation and accommodated individuals who might have had scheduling or geographical constraints.

The objective of using a focus group was to gain in-depth insights into the cybersecurity challenges facing the Australian healthcare sector, as identified by the participants. To facilitate the discussion, two researchers led the focus group. One acted as the convener, guiding the conversation, while the other researcher took detailed notes. This division of roles ensured that the flow of the conversation was well-managed, and no important points were overlooked.

The seating arrangement was designed to foster a comfortable and engaging environment. Two participants were seated around a table, while the other three joined remotely via Skype. This setup allowed for seamless interaction, and participants had equal opportunities to contribute to the discussion regardless of their physical location.

The structure of the focus group, as outlined in Table 4, followed a four-stage format designed to explore participant perspectives on cybersecurity and its impact on the Australian healthcare sector. The first stage was an introduction, which aimed to welcome participants, outline the session's objectives, and set expectations for the discussion. During this stage, the convener explained the purpose of the focus group, ensuring participants understood the topics that would be covered and the overall goals of the session. The introduction also helped establish rapport among participants, making them feel more comfortable and open to sharing their insights and experiences.

By utilizing both in-person and virtual formats, the researchers ensured that participants from various backgrounds and locations could be included, providing a diverse range of perspectives on the challenges and potential solutions for improving cybersecurity in the Australian healthcare sector. The interactive and structured approach allowed for an engaging exchange of ideas, contributing valuable insights into the current state and future needs of cybersecurity in healthcare.

Table 4 Structure of the focus group

Stage	Aim	Approximate Duration
-------	-----	----------------------

Introductions	Greetings, introduction of the facilitator, and the session's goal	10 minutes
Impact	Recognize participants' viewpoints regarding the impact of cybersecurity risks and solutions on the Indian healthcare industry.	30 minutes
Guided Expert	Find out how participants view particular cybersecurity possibilities and vulnerabilities' effects on the Indian	40 minutes

	healthcare industry.	
Wrap up	Highlight important points, pose closing queries, and express gratitude to participants.	10 minutes

The second phase examined participants' overall perceptions on how cybersecurity affects the Indian healthcare industry. Participants were invited to talk on how cybersecurity impacts healthcare professionals, consumers, and services by using open-ended questions.

The third phase changed to a more facilitated conversation. If they hadn't come out naturally in the second stage, the facilitator offered specific topics for participant feedback based on themes found in the cybersecurity and healthcare literature study. The effects of legacy systems, the development of medical devices, organizational and societal culture, media coverage of dangers, IT security funding and assistance, and the illicit market value of medical data were some of these subjects.

The purpose of this stage was to learn more about how participants thought these topics affected cybersecurity possibilities and vulnerabilities in the Indian healthcare system.

The final phase was a wrap-up. The discussion's main topics were outlined, giving participants a chance to double-check their comprehension and offer closing remarks. In order to gauge their early opinions, participants were also exposed to the idea of a healthcare cybersecurity index, which is a self-assessment tool for the Indian healthcare sector. The goal of this phase was to confirm the main conclusions drawn from the focus group.

It is noteworthy that the healthcare cybersecurity literature also served as the source of the indicative questions that were utilized in Stages 1 and 2 to direct the first round of open-ended conversations. This made sure the focus group remained thematically consistent and enabled a thorough investigation of participants' knowledge and experiences with cybersecurity in the Indian hospital setting.

Table 5 Indicative questions used in the focus group

Stage	Indicative Questions
Impact	From the perspectives of healthcare providers, professionals, and customers, how does cybersecurity affect India's healthcare industry?

Guided Impact	• What effect do you believe the following will have on Indian healthcare and cybersecurity? • What part do outdated technologies and legacy systems play? • the evolving field of medical technology, such as the rise in wireless medical equipment use? • Social culture or organizational culture? • The function of the media in covering cybersecurity and healthcare assaults and threats • Healthcare organizations' funding and assistance for IT security specialists? • Training, education, and professional growth? • The value of medical data on the "black market"?
---------------	--

With participant approval, the whole focus group session was audio recorded to guarantee thorough data collection for analysis. A detailed analysis of participant viewpoints and a deeper comprehension of the group's overall conversation were made possible by the verbatim transcription of the recordings.

The focus group's main purpose was to give participants a forum to talk about the broad weaknesses found in previous studies and literature in order to lay the groundwork. Second, a critical conversation about how these known vulnerabilities relate to the unique circumstances of Indian healthcare was facilitated by the focus group.

Findings

The conversations uncovered a complex terrain of potential and difficulties. The financial difficulties of cybersecurity, the necessity to strike a balance between privacy and transparency, the special vulnerabilities of the healthcare sector, and the function of legislation and education were among the major themes that surfaced. The participants also emphasized the limits of legacy systems, the serious lack of IT security experts, and the always changing danger posed by highly skilled cybercriminals. Both the advantages and disadvantages of the media's role in promoting awareness of cyberthreats were examined. Lastly, participants emphasized the necessity of a proactive cybersecurity strategy, highlighting the significance of readiness and constant watchfulness.

Table 6 Summary of the research findings

Theme	Summarised responses
-------	----------------------

The Indian healthcare landscape	
Difficulties	- Physical environment - Complex workflows - Data access complications involving several parties (government agencies, patients, and providers) - Software and legacy systems are still in use. - Private and public healthcare organizations have different priorities. - More and more medical devices are being linked to networks.
Usability and security in balance	- Healthcare workers' increasing knowledge of cyberthreats - Time limits for clinicians affecting security procedures (logging in/out) - Convenience-focused procedures (such as passwords that never expire)
Gaps in education and regulations	- Confusion and ignorance regarding data security among the general public - Laws that lag behind and find it difficult to adapt to new technologies
The financial challenges of cybersecurity in healthcare	
Allocating funds and resources	- Healthcare providers find it challenging to increase fees to pay cybersecurity costs. - Juggling the necessity of updates with financial constraints - Resources for continuous maintenance are limited by public funding schemes.

	- IT security is viewed as an indirect expense that competes with the demand for direct healthcare services. - The belief that cybersecurity measures are costly and might not be completely successful - Hiring IT security experts is expensive.
The weight of outdated systems	- Expensely updating antiquated systems because of interoperability issues - Legacy systems in the healthcare industry are a serious weakness.
Finding a balance between transparency and privacy	
Data security and privacy in balance	- The significance of protecting patient confidentiality and privacy - Possibility of improper use of patient data - Patient data is highly valuable on the illicit market.
Public conversation	- Media communication difficulties during hacks in the healthcare industry - The value of media attention in spreading knowledge and encouraging best practices - Transparency is essential for reducing harm and promoting discussion. - The role of public discourse in promoting social change

Data sharing and patient trust	- Public ignorance regarding the access and storage of healthcare data - People are choosing not to use electronic health records because they are afraid about cyberattacks.
Education and regulation	
Awareness and education of users	- Effective user education and training are crucial. - Cybercrime awareness in the media can encourage user education. - Users frequently don't comprehend the hazards associated with cybersecurity. - Sometimes, users put convenience ahead of security (weak passwords, for example). - Building a robust system is essential to reducing the impact of attacks.
The function of laws and regulations	- Clear legislation that outlines roles, responsibilities, and penalties for cybersecurity breaches is required. - The significance of a watchdog to guarantee adherence to cybersecurity regulations

Discussion

The results demonstrate the serious cybersecurity issues that the healthcare industry faces. Despite the security hazards, outdated systems continue to function because of their vital purpose and user familiarity. Upgrades are challenging due to limited funding, especially in public healthcare, which causes a gap with the commercial sector. This was noted in the focus group as well as in the literature. Critical vulnerabilities are created when IT infrastructure components, such as software and hardware, are not properly maintained and

upgraded. These vulnerabilities allow hackers to obtain sensitive healthcare data without authorization. Users' reluctance to update software, operating systems, and hardware can be attributed to a variety of causes, including the installation process, the cost vs advantages, and even a negative experience. The literature backed this up.

There may be disastrous repercussions from this lack of investment. It's possible that outdated software has known security holes that hackers might readily exploit. In a similar vein, aging hardware may break down and cause system failures or data breaches. Financial information and medical records may be made public by these breaches. In the worst situation, a hack might jeopardize patient safety by compromising patient data, delaying diagnosis, and impeding treatment plans. Coventry and Branley discovered that the high frequency of cybersecurity assaults in the healthcare industry was partly caused by the utilization of older systems.

Focus group participants emphasized the growing sophistication of hackers who can take advantage of any vulnerability, while others minimized the inherent risk of legacy systems. This means that in order to keep up with changing threats, security measures must be continuously invested in. IT security is further marginalized in budget allocation decisions due to its image as a "indirect overhead" as opposed to a fundamental clinical function. The possible financial repercussions of a cyberattack, which can be far higher than preventative measures, are ignored by this way of thinking.

The size and funding model of the healthcare organization can have a significant impact on the amount of money spent on cybersecurity technology, staff, training, incident response, and regulatory compliance. A tiny portion of their overall ICT budget or the amount allotted to this sector sometimes competes with healthcare service delivery. As the focus group highlighted, a complete strategy that incorporates both technological solutions and user training is necessary for effective cybersecurity. However, the continuous expense of security protocol maintenance and training can be demoralizing, which makes some users feel defeated. Unfortunately, the healthcare industry's financial difficulties are made worse by cyberattacks because of its high costs and low profit margins in comparison to other industries.

Allowing people to bring their own devices (BYOD) and integrating medical devices with networks (IoT) introduces new, unexpected attack areas. The focus group and the literature both backed this up. Some healthcare organizations' open environments make it challenging to regulate device usage and secure entry points, which runs counter to strong cybersecurity procedures. The sheer volume of users—from professionals to patients—who have access to data makes access management more difficult.

Internal healthcare organization policies and procedures, as well as legacy legislation, find it difficult to keep up with the rapid advancements in technology. Convenience is given priority in several contemporary practices, such as guest Wi-Fi and non-expiring passwords, which lead to vulnerabilities disguised as user-friendliness. Although it was believed that it was crucial to update current laws and regulations to take into account the changing nature of cyberthreats, questions were raised concerning the suitability of current standards and enforcement procedures.

Although participants acknowledged the significance of strong cybersecurity, they also emphasized the financial burden it places on healthcare organizations. This makes the cost of software updates, upgrades, and qualified IT security staff—who frequently go beyond cybersecurity budgets—difficult to pay. In light of the constantly changing panorama of cyber threats, participants also contended that more government funding is required because healthcare, particularly public healthcare, cannot handle these issues on its own.

The significance of patient privacy and data confidentiality is emphasized by Indian law. Participants do, however, recognize the significant value of patient data on the illicit market and the pervasive ignorance of the public about the storage and accessibility of healthcare data. Cyberattacks in the healthcare industry are surrounded by a culture of secrecy. Transparency, according to some participants, is essential for raising public awareness and promoting progress, but others are concerned that it would undermine confidence in the healthcare system.

The public is frequently informed about cybersecurity issues by blog entries, social media posts, and big media reports. When an incident happens, there may be a brief negative reaction (e.g., a brief decline in stock prices) once it is publicized in the public media, according to research done in other domains, like the stock market, but this does not persist. Wang et al. further hypothesized that the public had a more negative opinion of a security violation if it was ambiguous or thought to be "hiding."

The public's perception is greatly influenced by the media. Sensationalized media coverage can make patients worry about the security of their data, while open discussion about intrusions can compel reforms. Media coverage of cybersecurity events can have a big impact on prevention and education initiatives. Sensationalizing low-likelihood attacks can similarly skew perceptions of cybersecurity risk. Transparent media coverage of cyberattacks was seen as advantageous since it can increase public awareness, promote user education, and put pressure on decision-makers to take action.

The necessity of abandoning reactive tactics and adopting a more proactive approach to combating cyberattacks was emphasized by the participants. In order to guarantee that patients feel empowered and protected when interacting with personal health data, it was thought to be essential to educate individuals working in the healthcare industry about cyber dangers and best practices, as well as to communicate clearly and educate them about the advantages of programs like My Health Record. Implementing strong countermeasures that target user behavior in particular is essential because human behavior is frequently seen as the most weak point in an organization's cybersecurity defenses. Programs for education and training must be given priority because of this.

Conclusion

With the highest frequency of data breaches among all businesses, the Indian healthcare industry is increasingly vulnerable to cyberattacks. Vulnerabilities in healthcare cybersecurity have been further revealed by the move to remote work brought on by COVID-19. Cyberattacks in the healthcare industry can have disastrous results. While interrupted operations can make it more difficult to provide healthcare, compromised patient data can have a serious effect on individuals. Additionally, a cyberattack can have a huge financial impact, with budgets for healthcare being greatly impacted by costs ranging from data recovery to reputational harm.

The costly burden of maintaining antiquated systems, out-of-date laws, the dynamic nature of cyberthreats, and the complexity of the healthcare setting itself are all highlighted in this paper's exploration of these issues. It's difficult to strike a balance between patient privacy and public awareness of hacks. Transparency is essential for increasing public knowledge and promoting user education, but if not managed properly, it can also undermine public confidence in the healthcare system. Although sensationalized claims might cause fear and mistrust, media coverage of hacks can help increase awareness.

By highlighting the necessity of cybersecurity education for people working in the field and promoting empowerment, the paper underscores the need for a proactive approach to cybersecurity in the Indian healthcare industry. The industry would be better able to prioritize its cybersecurity resources and detect weaknesses with the creation of a customized self-assessment tool. A self-evaluation would also be helpful in defining "business as usual." For instance, does the healthcare company have a cybersecurity plan in place, do its staff members understand the risks associated with cybersecurity, and what kind of training is offered to help reduce and prevent risk? It may also provide the user with tactics to strengthen their defenses against cyberattacks and encourage self-efficacy, which is

the conviction that one must carry out the actions required to achieve success.

References

1. Frumento E. Cybersecurity and the Evolutions of Healthcare: Challenges and Threats Behind Its Evolution. In: Andreoni G, Perego P, Frumento E, editors. *m_Health Current and Future Applications*. Cham: Springer International Publishing; 2019. pp. 35–69. https://link.springer.com/chapter/10.1007/978-3-030-02182-5_4.
2. Le Bris A, El Asri W. State of Cybersecurity & Cyber Threats in Healthcare Organisations: Applied Cybersecurity Strategy for Managers. 2017. [Cited 2024 April 24]. <https://blogs.harvard.edu/cybersecurity/files/2017/01/risks-and-threats-healthcare-strategic-report.pdf>.
3. Australian Government. Notifiable Data Breaches Report: July-December 2021. 2022. [Cited 2024 April 24]. https://www.oaic.gov.au/_data/assets/pdf_file/0010/12205/Final-Notifiable-Data-Breaches-Report-Jul-Dec-2021.pdf.
4. Australian Government. Notifiable data breaches publications; 2023. [Cited 2023 April 25]. <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications>.
5. Australian Digital Health Agency. Annual Report 2017-18. 2018. [Cited 2024 April 24]. https://www.digitalhealth.gov.au/sites/default/files/2020-10/Annual_Report_Australian_Digital_Health_Agency_2017-2018_Online.pdf.
6. Australian Government. Notifiable Data Breaches Report: January to June 2023. 2023. [Cited 2024 April 24]. <https://www.oaic.gov.au/privacy/notifiable-data-breaches/publications/notifiable-data-breaches-report-january-to-june-2023>.
7. Australian Government. Notifiable Data Breaches Report: July to December 2023. 2024. [Cited 2024 April 24]. <https://www.oaic.gov.au/privacy/notifiable-data-breaches/publications/notifiable-data-breaches-report-july-to-december-2023>.
8. Australian Cyber Security Centre. 2020 Health Sector Snapshot. 2021. [Cited 2024 April 24]. <https://www.cyber.gov.au/about-us/reports-and-statistics/2020-health-sector-snapshot>.
9. Australian Cyber Security Centre. Ransomware targeting Australian aged care and healthcare sectors. 2020. [Cited 2024 April 24]. <https://www.cyber.gov.au/about-us/alerts/ransomware-targeting-australian-aged-care-and-healthcare-sectors>.
10. Australian Cyber Security Centre. ACSC Annual Cyber Threat Report - 1 July 2020 to 30 June 2021. 2021. [Cited 2024 April 24]. <https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Annual%20Cyber%20Threat%20Report%20-%202020-2021.pdf>.
11. Australian Digital Health Agency. Safe, seamless and secure: evolving health and care to meet the needs of modern Australia. 2017. [Cited 2024 April 24]. <https://www.digitalhealth.gov.au/sites/default/files/2020-11/Australia%27s%20National%20Digital%20Health%20Strategy%20-%20Safe%2C%20seamless%20and%20secure.pdf>.
12. Vora J, Nayyar A, Tanwar S, Tyagi S, Kumar N, Obaidat MS, et al. BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records. In: 2018 IEEE GC Wkshps. IEEE; 2018. pp. 1–6. <https://doi.org/10.1109/GLOCOMW.2018.8644088>.
13. Guo R, Shi H, Zhao Q, Zheng D. Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems. IEEE Access. 2018;6:11676–86. <https://doi.org/10.1109/ACCESS.2018.2801266>.
14. Chen Y, Ding S, Xu Z, Zheng H, Yang S. Blockchain-Based Medical Records Secure Storage and Medical Service Framework. J Med Syst. 2018;43(1):5. <https://doi.org/10.1007/s10916-018-1121-4>.
15. Jalali MS, Kaiser JP. Cybersecurity in Hospitals: A Systematic, Organizational Perspective. JMIRx Med. 2018 [Cited 2023 Jun 1];20(5):e10059. <https://doi.org/10.2196/10059>.
16. Abraham C, Chatterjee D, Sims RR. Muddling through cybersecurity: Insights from the U.S. healthcare industry. Bus Horiz. 2019;62(4):539–48. <https://doi.org/10.1016/j.bushor.2019.03.010>.
17. Bhuyan SS, Kabir UY, Escareno JM, Ector K, Palakodeti S, Wyant D, et al. Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. J Med Syst. 2020;44(98):1–

9. <https://doi.org/10.1007/s10916-019-1507-y>.
18. Rappaport J. In praise of paradox: A social policy of empowerment over prevention. *AJCP*. 1981;9(1):1–25. <https://doi.org/10.1007/BF00896357>.
19. Thomas JE. Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks. *IJBM*. 2018;13(6):1–24. <https://doi.org/10.5539/ijbm.v13n6p1>.
20. Nelson C, Soisson E, Li P, Lester-Coll N, Gagne H, Deeley M, et al. Impact of and Response to Cyberattacks in Radiation Oncology. *Adv Radiat Oncol*. 2022;7:1–7. <https://doi.org/10.1016/j.adro.2022.100897>.
21. Taylor J. Medibank v the hackers: how the health insurer fell to a mass data theft. 2022. [Cited 2024 April 24]. <https://www.theguardian.com/australia-news/2022/nov/12/medibank-v-the-hackers-how-the-health-insurer-fell-to-a-mass-data-theft>.
22. Morris-Grant B. Hackers have released stolen Medibank data on the dark web. What does this mean for customers? 2022. [Cited 2024 April 24]. <https://www.abc.net.au/news/2022-11-10/medibank-data-breach-latest-dark-web-leak/101632746>.
23. Rathke L. Hospital network reveals cause of 2020 cyberattack. 2021. [Cited 2024 April 24]. <https://apnews.com/article/technology-business-hacking-8e55983586642b30f77cfc4b4d87985e>.
24. Harrison JD, Auerbach AD, Anderson W, Fagan M, Carnie M, Hanson C, et al. Patient stakeholder engagement in research: A narrative review to describe foundational principles and best practice activities. *Health Expect*. 2019;22(3):307–16. <https://doi.org/10.1111/hex.12873>.
25. Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, et al. Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors*. 2021;21(15):1–25. <https://doi.org/10.3390/s21155119>.
26. Thompson C. Moving Forward for Cybersafe Healthcare: Insights from the Canadian Summit on Healthcare Cybersecurity [Report]. HealthCareCAN. 2018. [Cited 2024 April 24]. https://www.healthcarecan.ca/wp-content/themes/camyno/assets/document/Reports/2018/HCC/EN/CyberReport_final_web.pdf.
27. Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*. 2018;113:48–52. <https://doi.org/10.1016/j.maturitas.2018.04.008>.
28. Kirova D, Baumöl U. Factors that affect the success of security education, training, and awareness programs: A literature review. *JITTA*. 2018;19(4):56–83. <https://aisel.aisnet.org/jitta/vol19/iss4/4/>.
29. Halvorsen K, Dihle A, Hansen C, Nordhaug M, Jerpseth H, Tveiten S, et al. Empowerment in healthcare: A thematic synthesis and critical discussion of concept analyses of empowerment. *Patient Educ Couns*. 2020;103(7):1263–71. <https://doi.org/10.1016/j.pec.2020.02.017>.
30. Cartwright AJ. The elephant in the room: cybersecurity in healthcare. *J Clin Monit Comput*. 2023;37(5):1123–32. <https://doi.org/10.1007/s10877-023-01013-5>.
31. Stoumpos AI, Kitsios F, Talias MA. Digital Transformation in Healthcare: Technology Acceptance and Its Applications. *Int J Environ Res Public Health*. 2023;20(4):1–44. <https://doi.org/10.3390/ijerph20043407>.
32. Mahmoud R, Al Najjar Y. Cybersecurity in healthcare industry. *Glob Sci J*. 2024;12(2):978–85.
33. Clarke M, Martin K. Managing cybersecurity risk in healthcare settings. *Healthc Manage Forum*. 2024;37(1):17–20. <https://doi.org/10.1177/08404704231195804>.
34. Vilakazi K, Adebesein F. A Systematic Literature Review on Cybersecurity Threats to Healthcare Data and Mitigation Strategies. In: Gerber A, Hinkelmann K, editors. *Proceedings of Society 5.0 Conference 2023*. vol. 93 of EPiC Series in Computing. EasyChair; 2023. pp. 240–51. <https://doi.org/10.29007/hf15>.
35. Aldossri R, Hafizur Rahman MM. A Systematic Literature Review on Cybersecurity Issues in Healthcare. In: Smys S, Tavares JMRS, Shi F, editors. *Computational Vision and Bio-Inspired Computing*. vol. 1439 of *Advances in Intelligent Systems and Computing*. Springer Nature; 2023. pp. 813–23. https://doi.org/10.1007/978-981-19-9819-5_58.

36. Peve Herrera CV, Mendoza Valcarcel JS, Díaz M, Herrera Salazar JL, Andrade-Arenas L. Cybersecurity in health sector: a systematic review of the literature. *IJECS*. 2023;31(2):1099–108. <https://doi.org/10.11591/ijeecs.v31.i2.pp1099-1108>.
37. He Y, Aliyu A, Evans M, Luo C. Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. *J Med Internet Res*. 2021;23(4):1–18. <https://doi.org/10.2196/21747>.
38. Sardi A, Rizzi A, Sorano E, Guerrieri A. Cyber Risk in Health Facilities: A Systematic Literature Review. *Sustainability*. 2020;12(17):1–16. <https://doi.org/10.3390/su12177002>.
39. Crone D, Lozano-Sufrategui L. Interviews and focus groups. In: Bird S, editor. *Research Methods in Physical Activity and Health*. London: Routledge; 2019. pp. 80–92. <https://doi.org/10.4324/9781315158501>.
40. Krueger RA, Casey MA. *Focus groups: a practical guide for applied research*. 5th ed. Thousand Oaks: SAGE; 2015.
41. Liamputtong P. *Qualitative Research Methods*. 5th ed. Docklands, Victoria: Oxford University Press; 2020.
42. Morgan DL. *Basic and advanced focus groups*. Thousand Oaks: Sage Publications; 2018.
43. Patton MQ. *Qualitative research & evaluation methods: integrating theory and practice*. 4th ed. Thousand Oaks: SAGE; 2015.
44. Osman MC, Namukasa M, Ficke C, Piasecki I, OConnor T, Carroll M. Understanding How to Diversify the Cybersecurity Workforce: A Qualitative Analysis. *JCERP*. 2023;2023(2):1–12. <https://doi.org/10.32727/8.2023.23>.
45. Liu N, Nikitas A, Parkinson S. Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach. *Transp Res Part F Traffic Psychol Behav*. 2020;75:66–86. <https://doi.org/10.1016/j.trf.2020.09.019>.
46. Braun V, Clarke V. *Thematic Analysis: A Practical Guide*. UK: SAGE Publications; 2022.
47. Vitale F, McGrenere J, Tabard A, Beaudouin-Lafon M, Mackay WE. High Costs and Small Benefits: A Field Study of How Users Experience Operating System Upgrades. In: *Proc. CHI '17*. 2017. pp. 4242–53. <https://doi.org/10.1145/3025453.3025509>.
48. Gioulekas F, Stamatiadis E, Tzikas A, Gounaris K, Georgiadou A, Michalitsi-Psarrou A, et al. A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. *Healthcare*. 2022;10(2):1–9. <https://doi.org/10.3390/healthcare10020327>.
49. Lallie HS, Shepherd LA, Nurse JRC, Erola A, Epiphaniou G, Maple C, et al. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Comput Secur*. 2021;105:[20]. <https://doi.org/10.1016/j.cose.2021.102248>.
50. Wang T, Ulmer JR, Kannan K. The Textual Contents of Media Reports of Information Security Breaches and Profitable Short-Term Investment Opportunities. *J Organ Comput Electron Commer*. 2013;23(3):200–23. <https://doi.org/10.1080/10919392.2013.807712>.
51. Snider KLG, Shandler R, Zandani S, Canetti D. Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *J Cybersecur*. 2021;7(1). <https://doi.org/10.1093/cybsec/twab019>.
52. Burke W, Oseni T, Jolfaei A, Gondal I. Cybersecurity Indexes for eHealth. In: *Proc. of the ACSW Multiconference*. Sydney: ACM; 2019. pp. 1–8. <https://doi.org/10.1145/3290688.3290721>.
53. Hassandoust F, Techatassanasoontorn AA. Antecedents of IS infusion behaviours: an integrated IT identity and empowerment perspective. *Behav Inf Technol*. 2022;41(11):2390–414. <https://doi.org/10.1080/0144929X.2021.1928287>.
54. Bandura A. Self-efficacy: Toward a unifying theory of behavioral change. *Psychol Rev*. 1977;84(4):191–215. <https://doi.org/10.1037/0033-295X.84.2.191>.