# Indian Healthcare Demands Robust Cyber Security Infrastructure; Here's What Experts Say

It is crucial for healthcare organizations to invest in robust cybersecurity measures, including regular assessments, staff training, and the implementation of advanced security technologies, to protect against cyber threats


The healthcare sector has been experiencing a surge in cyberattacks, making it one of the most vulnerable segments due to the sensitive nature of the data they handle. Recent incidents such as the Sun Pharmaceuticals attack by the ALPHV Ransomware Group, AIIMS cyber-attack, and Safdarjung Hospital's hacking attack have put a spotlight on the need for stronger cybersecurity measures in the healthcare industry. These attacks not only compromise patient data but can also result in significant financial losses, disruption of operations, and damage to reputation.

**Most Vulnerable**

Healthcare is one of the most vulnerable industries, according to organizations offering cybersecurity solutions, due to the sensitive data they handle. Although it is hard to foresee the costs of a cyberattack on a healthcare organization. It is crucial for healthcare organizations to invest in robust cybersecurity measures, including regular assessments, staff training, and the implementation of advanced security technologies, to protect against cyber threats.

Sandeep Peshkar, Senior Vice President, Arete

The healthcare and pharmaceutical sectors have cybersecurity challenges since they deal with extremely sensitive and classified (PHI) data. It is crucial to strengthen defenses against these threats since the interconnectivity of devices and systems has increased the potential for data breaches.

As digitalization becomes a priority for every organization, enhancing security architecture is essential to protect customer data against ever-evolving threats. For example, last year, the Indian healthcare sector recorded 1.9 million cyber incidents. Moreover, how can we forget the recent AIMS cyber incident that compromised nearly 40 million health records.

In order to accomplish this, it is essential to develop a comprehensive cybersecurity strategy that includes policies, training, awareness activities, and technological safeguards. We can only secure the safety of people throughout the world and preserve pharmaceutical and healthcare data via collaborative efforts."

Parag Khurana, Country Manager, Barracuda Networks India

The healthcare and pharmaceutical industries are increasingly vulnerable to cyberattacks due to the sensitive nature of the data they handle. The biggest challenges to cybersecurity in these industries include the growing sophistication of hackers, the proliferation of connected devices, and the shortage of cybersecurity professionals. Our research finds healthcare (12 per cent) is one of the five key industries that ransomware attackers target.

To strengthen defenses against cyberattacks, healthcare and pharmaceutical organizations must implement robust security protocols, enhance employee security awareness training, and invest in advanced cybersecurity technologies. It's critical to recognize that cybersecurity is not just an IT issue, but a business-wide concern that requires a comprehensive approach.

As the stakes of cyberattacks continue to rise, there is an urgent need for healthcare organizations to adopt comprehensive cybersecurity solutions. Deploying a web application firewall is one of the most important steps to protect the organization, but it's just one part of a larger strategy:

· Prevent credential loss by implementing anti-phishing capabilities in email as email-borne threat is still the number one threat vector

· Secure applications and access with Multi-Factor Authentication (MFA) as well as implement web application security for all SaaS applications and infrastructure access points to protect against DDoS attacks or bad bots.

· Backup critical data with a secure data protection solution that help to implement disaster and recovery capabilities when needed.

Dr. Sanjay Katkar, Jt. MD; CTO, Quick Heal Technologies.

Healthcare organizations in India and globally are increasingly aware of the need to strengthen their cybersecurity posture due to the significant increase in cyberattacks targeting the healthcare industry. In the last 12 months, we have seen a significant increase in the number of hospitals purchasing security products, which is not surprising considering the growing number of cyberattacks targeting the industry. For instance, the cyberattack on AIIMS in November 2022 was one of the alarming attacks that shook the industry. This will continue as healthcare providers seek to safeguard patient data and ensure the continuity of critical services.

Further, Healthcare organizations are prioritizing the deployment of advanced security solutions in the coming months to mitigate the growing threat of cyberattacks and data breaches. One key area of interest is threat intelligence solutions that offer real-time threat detection and analysis capabilities. These solutions allow healthcare providers to detect and respond to threats quickly, staying ahead of cybercriminals and preventing significant damage.

Another area of focus is security analytics solutions that utilize machine learning and artificial intelligence to analyse large volumes of data and identify potential security threats in real time. By detecting patterns and anomalies that indicate a cyberattack, healthcare providers can take quick action to mitigate the threat. In addition, advanced identity and access management solutions are also being deployed to improve security posture by providing centralized control over user access to critical data and applications, reducing the risk of unauthorized access and data breaches