HealthManagement
Promoting Management and Leadership

More than 33% of Healthcare Organisations Aren't Prepared for Cyberattacks

Cybersecurity in the healthcare sector is facing unprecedented challenges, with a significant rise in cyberattacks that threaten patient care and data security. A recent survey by Software Advice highlights the severity of this issue, revealing that more than one in four ransomware attacks in healthcare impact patient care. This article explores the key findings of the survey and underscores the urgent need for healthcare organisations to bolster their cybersecurity measures. Software Advice's 2024 Medical Cybersecurity Survey was conducted online in March among 296 respondents working at healthcare organisations in the U.S. Respondents were screened to have IT management, data security, data management, or security training or audit responsibilities. Organisations that outsource 100% of their IT management or cybersecurity needs were excluded from participating.

The Growing Incidence of Cyberattacks

Over the past five years, there has been a staggering 256% increase in large breaches reported to the HHS Office for Civil Rights involving hacking. The survey indicates that over 30% of healthcare organisations have experienced a cyberattack in the last three years. Among these organisations, 42% reported experiencing a ransomware attack. These attacks often result in significant downtime, delaying critical medical procedures and compromising patient safety.

Impact on Patient Data and Care

The survey reports that about half of the healthcare organisations experiencing a ransomware attack noted an impact on patient data, with 34% failing to recover the data post-attack. Nearly half (48%) of ransomware attacks on medical practices specifically impact patient data, highlighting the sector's unique vulnerability compared to other industries. Furthermore, more than one in four ransomware attacks (27%) directly impact patient care, causing delays in critical procedures and access to medical records.

Lack of Preparedness and Response Plans

Despite the rising threat, only 63% of healthcare organisations have a cybersecurity response plan in place, leaving 37% without one. A cybersecurity response plan is crucial for a coordinated and efficient response to cyberattacks. It typically includes a formal definition of a cybersecurity incident, roles and responsibilities, communication protocols, and reporting requirements. Without such a plan, healthcare organisations may struggle to respond effectively to breaches, leading to prolonged downtime and increased data loss.

The survey also found that 55% of medical practices allow employees more access to data than necessary. This overexposure significantly raises the risk of data breaches, often caused by human error as much as by malicious attacks. Limiting data access strictly to what employees need for their roles can mitigate these risks.

Recommendations for Healthcare Organisations

To combat the increasing cyber threats, healthcare organisations must adopt several key strategies:

- Develop and Update Cybersecurity Response Plans: Organisations should create comprehensive cybersecurity response plans and regularly update them to address evolving threats. These plans should clearly define roles and responsibilities, ensuring that staff know exactly what to do during an attack.
- Enhance Employee Training: Effective training programmes are essential. In 2023, 74% of healthcare organisations spent fewer than five hours on IT security and data privacy training for their employees, with 35% spending two hours or less. Increased training can help staff recognise and respond to potential attacks, such as phishing scams.

© For personal and private use only. Reproduction must be permitted by the copyright holder. Email to copyright@mindbyte.eu.

- Restrict Data Access: Implementing user-based controls to limit data access is crucial. Network privileges should be restricted based on the role, and robust access policies should be enforced. This minimises the risk of unnecessary data exposure and potential breaches.
- Adopt Stronger Security Measures: Organisations should deploy advanced security measures, including network segmentation, to ensure that access to some data does not imply access to all data. Strong password protocols and regular audits can also enhance security.

The healthcare sector must recognise the critical importance of robust cybersecurity measures. With cyberattacks on the rise and the potential for significant impact on patient care and data security, healthcare organisations cannot afford to be complacent. By developing comprehensive response plans, enhancing employee training, and implementing stringent data access controls, the industry can better protect itself against the growing cyber threats. For those interested in improving their cybersecurity infrastructure, consulting with software advisors can provide valuable guidance and support.

Source: Software Advice

Image Credit: iStock

Published on : Thu, 30 May 2024

© For personal and private use only. Reproduction must be permitted by the copyright holder. Email to copyright@mindbyte.eu.