BDO USA

< Home < Insights < Industries < Healthcare

ARTICLE

April 12, 2024

BY:

Rajdeep Mukherjee
Director, Management Consulting

From Reactive to Proactive Cybersecurity Resilience in Healthcare

Healthcare as an industry was the biggest victim of ransomware attacks in the US in 2023[1]. As healthcare providers navigate complex challenges in protecting their digital environments, a significant concern arises. There is the tendency in the industry to pay for ransomware attacks, driven by the wealth of sensitive patient information it holds. While the rapid adoption of digital technologies has improved patient care and operational efficiency, it has also expanded the attack surface for cybercriminals. Common cyberattacks, such as cloud compromise, business email compromise, ransomware, and supply chain attacks, pose significant risks. These attacks not only threaten to breach sensitive patient data but can also disrupt vital healthcare services which can lead to negative patient care outcomes.

To address these cyber threats, healthcare leaders will want to prioritize identifying risks and vulnerabilities in third-party systems and outdated technology infrastructure, as well as emerging threats from generative AI. This advanced technology can aid in producing more convincing phishing emails and voice impersonations than ever before, making it a significant growing concern. It is becoming more critical for healthcare organizations to identify key organizational cybersecurity risks, understand the potential impacts of data breaches, and develop robust cybersecurity remediation plans alongside incident response capabilities. These plans should encompass both technological defenses and the human element. As cyber threats evolve, the repercussions are becoming increasingly severe and costly.

A Closer Look at the Numbers

The financial and operational impact of cyberattacks on the healthcare sector is staggering:

53%

The average cost of a healthcare data breach has now reached an unprecedented $11M, marking a 53% increase since 2020. – Healthcare Dive

88%

A concerning 88% of healthcare organizations reported experiencing a cyberattack in the past year. – Healthcare Dive

40m

Nearly half of the 40 million healthcare records exposed in 2023 were due to attacks targeting healthcare providers' third-party business associates. – Healthcare Dive

$346,667

Many HIPAA violations, which have led to financial penalties averaging $346,667 in 2023, stem from negligence and a failure to conduct comprehensive organization-wide risk assessments. – HIPAAJournal

BDO's Commitment to Cyber Resilience

At BDO, we recognize the importance of developing and implementing comprehensive defense in depth and cybersecurity risk management strategies to protect patient data and safeguard against the evolving cyber threat landscape. Our suite of Healthcare Cybersecurity and Compliance Risk Management Services is designed to proactively improve our client's cybersecurity posture and protect sensitive patient information. From organizational cybersecurity risk assessments and HIPAA compliance assessments to vulnerability assessments and penetration testing (VAPT), threat monitoring & detection, and incident response planning, our goal is to fortify your defenses and help improve the safety of patient data.

BDO’s Healthcare Trends & Topics Webcast Series

Cyber Defense in Healthcare: Are You Prepared for the Next Wave of Attacks?

Join us as we delve into the unique vulnerabilities of the healthcare industry, how to evaluate your threat profile, and steps to protect your organization to minimize the likelihood and impact of breaches and ensure the confidentiality, integrity, and availability of patient information.

Register Now