Healthcare Sector: CYBERSECURITY RISKS *(And How To Be Prepared)*

The healthcare industry is one of the most targeted industries, with ransomware and device compromise attacks on the industry hitting all-time highs. Unfortunately, given the expansion of cloud-based services, digital telehealth services, and the increase in the use of connected devices, these risks, if left unaddressed, are likely to contribute to even more compromised organizations.

Here's what you need to know to stay protected.

WHY THE HIGH RISK?

Minimal resources:
The healthcare industry invests less than 6% of its budget on cybersecurity. The finance industry, for example, another highly targeted industry, spends around 10% on cybersecurity.

Outdated software and systems:
According to one study, 83% of medical imaging devices are running on unsupported operating systems.

IoT devices and telehealth:
53% of connected devices are at risk of a cybersecurity attack with IV pumps (38% of a hospital's IoT footprint) and VoIP systems (50%) being the most vulnerable.

This makes for a very risky landscape for healthcare organizations who are already lacking the appropriate resources and may not be prioritizing cybersecurity in their future plans.

COMMON ATTACKS

Ransomware:
Ransomware is a huge risk for healthcare organizations particularly due to the urgency involved with such an attack. Hackers know that there's an urgency to bring operations up as soon as possible or risk affecting their in-house patients.

Device compromise:
The use of IoT and connected devices has increased healthcare company's attack surface. IT leaders may not always prioritize device security and some devices have known default passwords that can be exploited.

Unsecure or misconfigured databases:
The shift to telehealth is part of a larger push into digitization and use of cloud-based, third-party infrastructure and services. However, without any security in place, there's a lot of room for error, accidental exposure, and risk of data breaches.

Data Security and Compliance:
Given the new push into digital services, HIPAA compliance has become much more complicated for many organizations.

IN THE NEWS

Attacks are costly:
The average cost of a data breach for a healthcare organization is $10.1M, a record high for the industry.

Fines are no joke:
GoodRx, an online healthcare service provider had to pay $1.5M in penalties due to violating multiple regulations associated with health data sharing, and user tracking.

HCA was hacked:
HCA Healthcare was recently hacked, compromising data on over 10M patients, including personal details as well as a person's last patient visit.

HOW THE HEALTHCARE INDUSTRY CAN BE PREPARED FOR CYBER RISKS

Invest more in cybersecurity:
Cybersecurity needs to be a priority alongside a digital transformation strategy. This includes ensuring implementations and integrations are done securely and also vetting vendors and third parties through a security lens.

Device and network security:
IT leaders should ensure that devices have some form of security available and that any default passwords are changed to minimize unauthorized access.

Data protection and security practices:
Prioritizing data security and protection will help organizations better adhere to compliance and regulatory standards, while also providing information related to any audit or investigations.

HAVING A MANAGED SECURITY PROGRAM PARTNER:

Having the proper security in place is likely an expensive endeavor that will take several months (at the minimum) to implement. A more cost-effective and faster solution is for a company to partner with a managed security program provider. This is essentially a cybersecurity partner that provides 24/7 coverage, expertise to ensure compliance adherence, and guidance that will help your company find the right tools and systems to defend against potential risks.

Don't wait for a cyberattack to disrupt your operations. Take action now to secure your infrastructure and safeguard your organization. Reach out to SolCyber, the experts in cybersecurity for the healthcare sector, and start building your cyber resilience today.

Take Action Now

SolCyber

solcyber.com