PROACTIVERISK

A Case for Cybersecurity

The Medical Diagnosis for the Healthcare Industry

Hackers often target the healthcare industry for a litany of reasons—they are critical infrastructures that perform life-saving duties, house loads of personal and financial data, and are often wirelessly connected to affiliate locations. The need for healthcare institutions to stay in business every day is critical for the health and safety of those in our community. With that in mind, hackers take advantage of the industry's lack of IT talent, competing priorities, financial constraints, and use of outdated systems. These vulnerabilities can lead to successful attacks, impacting the livelihoods of patients and staff.

The Threat at Hand

According to research in the last year:

Healthcare: #5 in the top global industries targeted in 2022.

M-Trends

Healthcare: #7 in the top number of incidents and #4 in the top percentage of incidents that became successful breaches.

Top patterns included:

- Secretly getting into the computer systems
- Maliciously using web applications
- Accidentally sending data where it shouldn't go

Verizon

The 10 largest healthcare breaches in 2023, as of 7/5/23, have affected more than 30 million Americans.

Chief Healthcare Executive

If a cyberattack on the healthcare industry is successful, it can lead to:

- An inability to access electronic patient records
- The inability to use systems
- The required diversion of patients
- The release of sensitive information

Regaining control and recovering from an attack has substantial costs, including credit monitoring and identity theft services for the victims of leaked data.

This data may include personal information, financial information, and/or medical records for patients and staff spanning decades.

Regaining control and recovering from an attack has substantial costs, including credit monitoring and identity theft services for the millions of victims with leaked data. Unfortunately, the following businesses know this experience too well.

- Managed Care of North America, **a dental insurer**, was hit with the largest breach of health data thus far in 2023, affecting more than **8.8 million Americans**.
- Cerebral, Inc., **a telehealth company**, had "patient information… inadvertently disclosed to other parties," affecting more than **3.1 million people**.
- PharMerica, **a pharmacy services firm**, was hit with a cyberattack in March, affecting more than **5.8 million Americans**.
- Community Health Systems, **a Tennessee-based hospital system**, was affected by a cybersecurity incident, impacting **960,000 people**.

Five Tips to Keeping Threats at Bay

So, what can you do to prevent these cyberattacks? Hackers must be prevented from halting critical services and negatively impacting your ability to maintain the health and safety of patients across the country. **Here are our top five tips:**

TIP #1

Enforce cybersecurity best practices for all staff

TIP #2

Back up your data and encrypt it so there are usable copies that hackers can't read it

TIP #3

Develop a plan for if and when a security incident occurs

TIP #4

Partner with a cybersecurity vendor that can quickly detect unusual data access

TIP #5

Enforce secure device management

Your Partner in Protection

As a managed service provider, we provide IT and cybersecurity services to a variety of businesses, including those in the healthcare industry. We are backed by an elite, 24/7 security operations center that provides us with visibility, around-the-clock protection, and intel to drive best practices. Together, we can ensure hackers don't halt your medical facility's operations. Harness our experience protecting healthcare companies to better defend you and your patients.

Get started today by contacting me via phone or email.

PROACTIVERISK

9732981160 | sales@proactiverisk.com | www.proactiverisk.com