


Cyberattacks are taking a toll on healthcare systems and hospitals. Although these types of attacks are not a new phenomenon, the number of incidents has increased dramatically in the past few years.

Intracorp estimates that the average cost of each breach is around \$10 million, making healthcare the fastest growing industry to experience multi-million-dollar penalties.

The attacks are not only jeopardizing patient safety and privacy but the financial toll is wreaking havoc on many of these healthcare institutions.

Intracorp highlighted a few recent attacks that resulted in huge financial losses. In October 2022, CommonSpirit Health, the largest Catholic health system in the U.S., was the victim of a cybersecurity attack that resulted in more than \$150 million in losses from legal fees, data breach mitigation and more.

And in May 2021 Scripps Health, a non-profit healthcare system based in San Diego, CA, was the victim of an IT system attack that resulted in their patient portal being offline. The company said in its annual earnings report that it estimated lost revenues to be \$91.6 million plus additional costs related to the incident were estimated to be at \$21.1 million.



According to cyber security group **Intracorp**, healthcare organizations worldwide averaged **1,463 cyberattacks per week in 2022, an increase of 74% compared with 2021**. And in just the first half of 2023 alone, there have been **295 healthcare data breaches**, according to the U.S. Department of Health and Human Services Office for Civil Rights.

Be Proactive

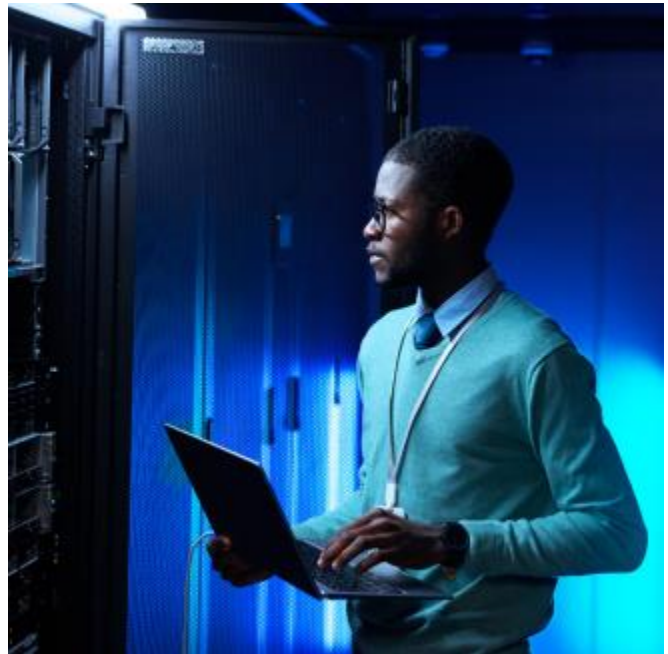
What can health systems do to protect themselves?

Healthcare IT environments can be complicated to defend against cyberattacks because patient information has more privacy and protection requirements than other type of data. Nevertheless, experts say that to combat the increasing number of these cyberattacks combined with the growing sophistication of the incidents, healthcare companies must take steps to reduce their risk.

They can do this by making cybersecurity a top priority. While it's important to proactively train employees on the importance of cybersecurity, it's also critical to invest in the necessary tools and technologies to prevent attacks. Without a good foundation, companies will remain at high risk for these attacks.

Frontier's Managed Network Services (MNS) combined with Managed Security serves as that foundation for companies because it protects sensitive healthcare data and helps fortify the customer's network against malicious attacks.

Frontier's Managed Security, part of the Managed Network Services (MNS) portfolio, provides a trusted firewall to protect against online threats, client VPN for secure remote file access and instant notifications in the event of any potential security threats.



Managed Network Services for Reliable Performance and Secure Networking

At the core of MNS is Managed Dedicated Internet, which delivers 99.99% guaranteed circuit availability and speeds as fast as 1 Gbps. Managed Dedicated Internet is installed, configured, monitored and managed 24/7 by Frontier's team of technical experts.

Frontier's Managed Cellular Failover, a service enhancement to MNS, will automatically failover the business' internet connectivity to a secondary cellular connection if the Managed Dedicated Internet service goes down. Managed Cellular Failover also provides unlimited data, optimized cellular signal coverage, and encryption so that data is protected during the outage.

Another service enhancement of Frontier's MNS is Managed Wi-Fi, which provides a fully managed, robust indoor/ outdoor Wi-Fi coverage (up to 10,000 square feet), separate private and guest Wi-Fi networks with a customizable guest log-in screen and guaranteed security for all end users.

All of Frontier's MNS—Managed Dedicated Internet, Managed Cellular Failover, Managed Wi-Fi and Managed Security — are closely monitored with a single-pane-of-glass dashboard that offers visibility into the entire MNS environment. This dashboard allows customers to see bandwidth utilization across the network. Being able to monitor usage and network performance this closely lets companies decide when to be proactive about increasing or decreasing bandwidth. Frontier's MNS is powered by Cisco Meraki, operator of the industry's largest-scale cloud networking service and a Gartner Magic Quadrant leader.

Reducing Risk

Reducing the risk of cybersecurity attacks is a huge priority for healthcare companies today. By investing in the right tools and technologies and partnering with trusted partners, healthcare organizations can take an important step toward reducing their risk.

Ready to learn more? Discover how Frontier's [Managed Network Services](#) can help your business improve operational efficiencies.