The Vital Role of Cybersecurity in Safeguarding Healthcare

ARTICLE 08.09.23 GUI COZZI

A federal class-action lawsuit was filed in the U.S. District Court Western Kentucky District of Kentucky Louisville Division against Norton Healthcare on behalf of employees and patients whose personal information was stolen from Norton's servers in a cyber attack earlier this year.

Cyber attacks on healthcare systems and providers of all sizes have seen a sharp uptick since the beginning of the COVID-19 pandemic. Threats continue to grow as the number of connected devices across more networks increases. Combined with cloud services gaining in popularity, this creates a larger attack surface for bad actors constantly evolving the sophistication of their efforts. Everything from patient admissions information and payment records to private electronic health records (EHRs), e-doctor visits, medical device wearables, and portable medical technologies can all be susceptible to compromise.

But a healthy cyber security posture can help defend against more than just an attack on a network, devices, or even an organization's reputation: It can aid in protecting the most vulnerable among us.

By understanding the challenges at hand and putting mitigation efforts in place, healthcare providers can work toward the all-important triad of confidentiality, integrity, and availability of information. Meanwhile, they ensure access to vital patient data at the most crucial moments in the continuum of care.

The Most Common Healthcare Cyber Threats

As the technology we rely on to deliver cutting-edge care continues to advance, so too do the complexities and stealth of cyber attacks.

The most common purpose of an attack, as we've noted, is accessing sensitive information to either sell or for personal use. The methods of these attacks, however, can be as varied as the attackers, including destruction of data and industrial espionage.

In the context of healthcare cyber security, here are a few threats causing the greatest damage to bottom lines — and reputations.

Ransomware

When a machine or a device is infected by ransomware, the files and other data are typically encrypted, access is denied, and ransom is demanded. Patient care services are particularly vulnerable to this type of attack due to their high dependence on technology combined with the critical nature of their daily operations. In fact, ransomware attacks on the sector occurred at a rate of four incidents per week in the first half of 2021.

Health records are a low-risk, high-reward target for cybercriminals because each record can fetch a high value on the underground market. Unfortunately, ransom payment doesn’t always result in the return of the stolen information.

Phishing

Many significant security incidents are caused by a variety of phishing attacks. The effectiveness can be attributed to criminals targeting the weakest link in the cyber security chain: people. Unwitting users may click on a malicious link or open a malicious attachment and infect their computer systems with malware that ultimately divulges information or enables access to it.

Cloud Storage Threats

Many healthcare providers have been switching to cloud-based storage solutions for greater convenience, and an “always on” connectivity. Unfortunately, not all cloud-based solutions are HIPPA compliant, making them easy targets for intruders. Threats include improper access management, data breach, data leak, loss of sensitive data, and misconfiguration of cloud storage. What’s more, some organizations don’t properly encrypt the data — or implement restrictions — before transmitting.

Be sure to utilize a private cloud or an on-premise data center to regularly secure and encrypt data.

Internal Threats

In our high-level primer on cyber security, we share research indicating that 90% of cyber claims stem from some type of human error or behavior. As more healthcare professionals access sensitive patient information on more devices — some which are still unsecured — the likelihood of an attack increases. While some internal threats can be malicious, most are the result of negligence or unwitting compromise.

Give your healthcare organization a first step in the right direction to mitigating risks, safeguarding your valuable data, and protecting your reputation. Connect with Dean Dorton for a cyber security risk assessment today.