Fighting Cyber Attacks - 5 Ways Healthcare Organizations can Protect Their Data

Cybersecurity has long presented a challenge for the healthcare industry. In 2015, over 113 million records were compromised; more than the previous 6 years combined.

The challenge increased in 2020, the overall rise in cyber-attacks because of the COVID-19 pandemic resulted in over 28,756,445 healthcare records compromised. 2020 became the third-worst year for healthcare record breaches.

Most Common Healthcare Cyber Attacks

Valuable patient data and the propensity to pay off ransoms rather than risk lives make the health industry a valuable target for cybercriminals. Below is a brief overview of the most common cyber attacks affecting the healthcare industry today.

1. IoT Exploits

According to this 2019 report, 82% of healthcare facilities have been targeted by an IoT device attack. While wearable IoT healthcare devices bring advantages, existing medical devices, like pacemakers and monitors, often have outdated operating systems that cannot support security applications.

Newer IoT devices come with more security features, but it might take years for healthcare facilities, often reluctant to move away from familiar legacy systems, to replace older medical devices with more secure ones.

2. Ransomware

Ransomware is a type of malware hackers use to hold important computer files hostage for a ransom. Personal health information is valuable, making the healthcare industry an attractive target for ransomware. A recent attack on the University of Vermont Health Network rendered its patient portal inaccessible and knocked out electronic communications across the main medical center.

Hackers know that a hospital is more likely to pay a ransom to avoid putting patients at risk. Cybersecurity Ventures predicts ransomware could cost 57 times more in 2021 than in 2015.

3. Unsecured mobile devices

The number of new mobile malware variants increased by 54% in 2018, indicating that mobile devices are becoming a larger threat landscape for cyber attacks. In recent years, healthcare employees have been using the same mobile device for both work and personal use. A SkyCure report found that 65% of doctors use instant messaging on their mobile devices to share patient data.

Weak mobile device passwords, failure to install security updates, and inadequate Bring Your Own Device (BYOD) policies could mean that your employees are accessing patient information from unsecured devices.

4. Medjacking

Medjacking or medical device jacking is a cyber attack that takes advantage of unsecured medical devices to create backdoors into a hospital's network. Many medical devices run on outdated operating systems like Windows XP which provide little or no threat detection support.

Because devices like MRI machines and ventilators are integrated into the hospital's computer system, cybercriminals can manipulate these devices to access vital patient information and find passwords to gain entry to other areas of the system.

A successful medjacking attack could jeopardize a patient's life if it results in a misdiagnosis or medical device malfunction.

5. Phishing

Phishing is often the initial entry point into a company's system and can occur via email (most common form), websites, social media, and SMS messaging (smishing). Emails that appear urgent or work-related encourage the recipient to take urgent action by downloading an attachment or clicking on a link.

In November 2020, employees at Massachusetts hospitals received emails that appeared to be from the Department of Health and Human Services requesting COVID-19 statistics. The attempt was unsuccessful but caused the institution to implement tighter email security controls.

A busy healthcare worker checking email on the go may not think twice about responding to an email from an apparently trusted source. They could unknowingly create a vulnerability that puts the healthcare facility at risk.

5 Best Practices for Healthcare Data Security

1. Restrict Access to Applications and Data

Hackers take advantage of vulnerabilities in your network created by employees with incorrect levels of access. To minimize this risk, only authorized persons should be able to access the company's sensitive data, applications, and devices.

Data access levels assigned should only be enough for an employee to carry out their day-to-day job functions with additional access requested as needed. Multi-factor authentication should also be enforced to verify user identity when attempting to access patient data.

2. Log and Monitor Use

Logging and monitoring data usage allows you to see how users are accessing the organization's resources. Centralized management tools are useful for monitoring user activity and identifying suspicious activity in real-time. Data monitoring tools can also be used to data usage policies related to emails and data transfer.

Monitoring logs in real-time can help you see where users are logging on from and how data is being transmitted. They are also a valuable resource during network security audits and can be used to identify vulnerabilities and risks in the security network.

3. Encrypt Data

Data encryption is one of the most effective ways to mitigate the risk of data breaches. While data encryption does not prevent an attacker from accessing your data, the data is practically useless unless it is deciphered. Both stored and in-transit data should be encrypted, including emails and data stored on hard drives, mobile devices, or in the cloud.

Encrypted data is a HIPAA compliance requirement and could result in thousands of dollars in fines if not implemented.

4. Backup Data to a Secure, Offsite Location

The threat of ransomware attacks alone should drive home the importance of having viable data backups. Hackers know that healthcare facilities are more likely to pay a ransom, rather than put a patient's life at risk.

Most cloud-service providers offer secure backup and recovery solutions to their offsite data centers. Backups stored in the cloud ensure that you can quickly restore important patient data if it becomes inaccessible, whether by a cyberattack or natural disaster.

5. Conduct Risk Assessments on a Regular Basis

Security risk assessments can identify vulnerabilities and weaknesses in your organization's security controls. A security risk assessment a proactive measure used to identify vulnerabilities and risks in your business' infrastructure and policies.

Because data risks can change over time, risk assessments should be conducted at periodic intervals. The results of your security risk assessment should be used to create a plan to mitigate risks to your organization

Contact [redacted] for your Security as a Service Needs:

Inadequate security controls in your healthcare institution could result in compromised patient health data and costly fines. [redacted]' Security as a Service solutions (SECaaS) can help you protect your data, networks, and end-point devices against cybersecurity threats.

Contact us today for more information about our services.