BANK OF AMERICA

Staying safe in a world of healthcare data breaches

Healthcare organizations have become frequent targets of cybercriminals, putting organizations and their patients, employees and communities at risk. According to a 2018 analysis by Thales Security, 77% of U.S. healthcare organizations have reported experiencing a data breach, and 48% of organizations say they have been breached in the past year.[1] Healthcare providers must not only care for patients and communities, but also understand how to protect an increasing number of electronic records, online portals and connected devices. Here are solutions that can help protect your organization and help you combat fraud when it occurs.

AUTHOR

John Hesselmann
National Head of Healthcare
Bank of America

Common types of attacks and breaches

Healthcare organizations face the same universal cyber fraud incidents seen by all businesses, across all industries. There are three main fraud cases that put healthcare organizations at risk:

1. **Unauthorized access of treasury** — Occurs when criminals gain access to an organization's treasury or employees' financial information to trick the system into sending a check or payment for a nonexistent transaction, or persuade an employee into wiring a payment to a fraudulent bank account.
2. **Malware/ransomware installed** — Occurs when criminals try to install malware onto an organization's computer network, demanding a ransom to restore the system and its data to normal operations.
3. **Theft of personal info** — Occurs when hackers break into an organization's database of information to steal the personal, medical or financial information of patients and employees.

How can you protect your patients, your organization and your employees against cyber fraud? Here are a few approaches to help make your data and systems safer and more secure:

1. **Protect your data.** Hospitals have become a key target for cyberattacks because they hold large volumes of valuable information — from patient and employee records to the information used to access corporate bank accounts and insurance monies. Legacy IT issues often make healthcare organizations particularly susceptible to cyber fraud. To protect your data, healthcare providers need a data storage plan and policies for data retention, privacy and disposal that extend across the entire organization.

2. **Keep your systems safe and up to date.** As patient records are migrated from paper to digital, organizations need to be vigilant in keeping track of records and how they are handled. This involves regularly backing up data stored in computer systems and installing firewalls to limit employee internet access while on the system. Organizations should also create a software management plan that includes checking for software updates, updating antivirus software and installing software patches on a regular basis to keep records and systems safe at all times.
3. **Teach employees to recognize and handle potential fraud.** In 2017, total damages from data breaches cost the industry $6.2 billion, according to Protenus.[2] Data breaches are often accomplished via old-fashioned and low-tech phishing techniques. The most well-meaning employees can make an error in judgment by clicking on a link or responding to a fraudulent email that ends up creating a system-wide problem. Employees need training on how to recognize phishing emails and understanding their potential consequences. One way to keep staff alert is to test them by periodically sending out fake phishing emails.
4. **Create policies that support cybersecurity efforts.** Organizations don't always have a cybersecurity chief in place, and many have yet to establish solid policies to protect computer systems and data. To support cybersecurity health within an organization, establish data protection policies for employees working off-site and institute a clear policy for professionals bringing their own devices into a facility, especially when those devices are used to access patient or hospital data. Organizations can also implement dual approvals as a requirement for any significant financial transactions to avoid confidential information being intercepted by cyber criminals.
5. **Keep your vendors on the same page.** A strong vendor management program includes regularly checking the data protection policies and procedures of vendors, third-party services and strategic partners to make sure everyone has necessary levels of cybersecurity in place. To keep everyone aligned, review your vendors' cybersecurity policies to find out if your system is affected if their systems are breached and then develop clear vendor policies, including guidelines for access to information, data security, liability and loss recovery.
6. **Be prepared for a fraud event.** According to Bank of America, 90% of fraud attempts come through phishing emails directed at an organization's weakest link: its users, who are often unaware and unprepared.[3] One of the most effective preparation tools is a tabletop exercise that can walk the organization through a simulated ransomware event. Organizations should construct a plan to deal with fraud events, ransomware and other situations that affect data and potentially freeze the system.
7. **Stay informed.** To get ahead of cybersecurity threats overall, organizations can stay updated on the newest types of cyber threats and criminal activity by monitoring trade publications and business news, and by keeping in touch with partners who have a global view of fraud across markets and industries.

By staying up to date on cybersecurity trends in the news, educating all members of the organization and preparing for a potential threat, healthcare organizations can protect patient data and care, successfully maintain the trust of the public and the organization's reputation, and combat fraud when it occurs. Healthcare companies must understand the risks and take precautions to protect their patients, employees and communities.

BANK OF AMERICA

[1]Thales Healthcare Data Threat Report, 2018.
[2]Protenus, Cost of a Breach: A Business Case for Proactive Privacy Analytics, 2017.
[3]Bank of America Merrill Lynch, Fighting Fraud: How Healthcare Organizations Can Stay Safe, 2018.