RISK INSIGHTS

NAVIGATING CYBERSECURITY CHALLENGES IN THE HEALTH CARE INDUSTRY

Cybercriminals often look to industries they can exploit, and there are several reasons they target health care providers, including:

- **Valuable data**—Health care organizations store extensive personal and medical information, including Social Security numbers, medical histories and insurance details. This data can be exploited for identity theft and financial fraud.
- **Critical operations disruptions**—Health care providers offer vital care, so disrupting their operations can have immediate and severe consequences. These factors make health care organizations appealing targets for ransomware attacks, as malicious actors may believe these facilities are more likely to give in to the cybercriminals' demands to restore operations swiftly.
- **Vulnerable infrastructure**—Health care providers may still rely on outdated and unpatched legacy systems, creating exploitable weaknesses. Additionally, complex networks with the proliferation of IoT devices, cloud-based systems, telehealth services and third-party vendor integrations expand the attack area and entry points for cybercriminals, making organizations more vulnerable to attacks. Furthermore, staff often have not received sufficient training and lack cybersecurity awareness, increasing susceptibility to phishing attacks, human error and unintentional data leaks.

COMMON TYPES OF CYBERATTACKS

Cybercriminals utilize several methods of infiltration. The following types of cyberattacks are common in the health care industry, each with a different purpose and impact:

- **Ransomware attacks**—These cyberattacks occur when a cybercriminal installs malicious software on an organization's network that encrypts critical data. The attackers then demand payment in exchange for decryption. Ransomware attacks are utilized for quick financial gain and to disrupt or halt operations. If a health care provider falls victim to such an attack, patient care may be delayed, and reputational harm and financial losses may also occur.
- **Phishing attacks**—This type of attack involves malicious actors tricking users into providing sensitive data or login information through fraudulent emails, text, calls, websites or links. Health care providers may not be adequately trained to identify these phishing attempts, and cybercriminals can exploit this unfamiliarity, tricking them into revealing confidential information or clicking on malicious links. Victims of phishing attacks may have their identities stolen.
- **Data breaches**—Hackers can gain unauthorized access to patient records and commit large-scale data theft, compromising their privacy and leading to legal consequences and regulatory fines. This can be done by physically accessing a network or breaching network security measures. Additionally, individuals with authorization to access an organization's data—including employees and business partners—can intentionally or accidentally release sensitive information, sabotage systems or facilitate attacks.

RISK INSIGHTS

- **Distributed denial of service (DDoS) attacks**—These happen when cybercriminals overload a health care organization's network with traffic, disrupting care delivery or causing a network outage, leading to significant delays. The cybercriminals can then leverage the interruption to extort a payment from a health care provider in exchange for ending the DDoS attack.
- **Exploitation of Internet of Things (IoT) vulnerabilities**—If not properly secured, connected medical devices can serve as entry points for cybercriminals, jeopardizing patient safety and data integrity. Cybercriminals can infiltrate an organization through weak points in the IoT network. When this type of attack occurs, it can create care disruptions, financial repercussions and a loss of client trust.

CYBERSECURITY BEST PRACTICES

To help combat cybersecurity risks, health care industry leaders should bolster their digital defenses. In particular, they should:

- **Conduct regular risk assessments**. Scheduling routine and thorough cybersecurity risk assessments with penetration testing can help find weak points in networks, systems and processes before they are exploited. Health care providers should establish response plans to remedy any discovered vulnerabilities.
- **Provide robust cybersecurity training and vet employees**. Employees should undergo a background check before they are hired and granted access to sensitive information. Once on the job, they should receive regular training on cybersecurity best practices as well as applicable regulations (e.g. the Health Insurance Portability and Accountability Act). This also fosters a culture of security, encouraging employees to report suspicious activities.
- **Patch software and utilize technology**. Installing advanced antivirus and malware protection software and using patch management systems to ensure software updates occur can help prevent malware from infecting systems. Technologies such as AI and machine learning can also be leveraged to detect unusual activity within a system to stop an attack and prevent it from spreading.
- **Segment networks and use firewalls**. Segmenting networks and utilizing firewalls can limit malicious actors' access to sensitive information.
- **Encrypt data**. Data encryption transforms data into an unreadable, encoded format so that cybercriminals cannot decipher it without the key. Sensitive data should be encrypted both in transit between networks and while at rest or stored to protect it from unauthorized access.
- **Establish access controls**. Strict access controls should be enforced for all employees. These could include multifactor authentication, which requires users to provide at least two forms of verification to access data and devices. Permission to access data and devices should be based on roles and responsibilities to minimize unauthorized access.
- **Vet third-party partners and have a cyber incident response plan**. Selecting and working with partners with strong cybersecurity defenses can mitigate the risk of a hacker accessing a health care provider's network through a third-party cyber vulnerability. A well-prepared cyber incident response plan can further address cyber risk by instructing organizations on how to respond swiftly to attacks and minimize their impact.

RISK INSIGHTS

ROLE OF CYBER INSURANCE IN MITIGATING RISK

Cyber incidents can still occur even with robust cybersecurity measures in place. Cyber insurance can mitigate a health care provider's exposure to cyber-related damages by covering losses arising from cybersecurity incidents. It can also provide financial assistance for data recovery costs, legal liabilities and operational interruptions resulting from a cyberattack. Importantly, some insurers require minimum cybersecurity measures before offering coverage. Cyber insurance complements rather than replaces strong cybersecurity practices.

Many cyber insurance policies provide access to a vendor panel with public relations firms, legal counsel, IT specialists and other experts who are experienced in risk assessment techniques and cyber incident management. These experts can assist in navigating the complex and evolving regulatory landscape and provide tips on strengthening cyber defenses. They can also enable health care providers to respond quickly and effectively to reduce a cyber incident's impacts should one occur.

Cyber insurance policies vary in coverage, limits and exclusions. Consulting a licensed insurance professional can help health care providers to select the best policy to meet their needs.

CONCLUSION

The health care industry faces several cyber risks due to the nature of its operations and the information it processes and stores. Implementing robust cybersecurity protocols and securing a well-chosen cyber insurance policy can help health care leaders address these exposures and safeguard their businesses' operations, data, finances and reputations.

For more risk management guidance and coverage solutions, **contact us today.**