Cybersecurity in Healthcare

Background

Few industries make better targets for cybercriminals than healthcare service providers. These organizations are responsible for maintaining personal and patient health information (PHI), some of the most sensitive information available and, therefore, some of the most valuable information targeted by ransom attacks. Patient files also contain marketable personal identity information, including dates of birth, street and email addresses, credit card and other financial information, Medicaid and Medicare account information, and social security numbers.

The business impact of these cyber incursions is significant and the fallout from a cyber breach for a healthcare organization can be severe due to the loss of trust, reputational damage, financial cost, and patient suits. The most damaging aspect of cyber breaches for a healthcare organization is how IT system downtime impacts operational downtime and patient care.

Unfortunately, the risk of cyberattacks is increasing. Each year, healthcare providers collect, store (often in the cloud), and share an increasing volume of information, thanks to additional software solutions, mobile apps, and devices connected to the Internet of Things. This all adds up to more data and more points of entry into the data-related systems of these service providers.[1]

Hazards Contributing to the Risk

Hazard 1: Failure to Follow Best Practices for Reviewing Vendor Supply Chains

Through the first half of 2021, 60% of reported healthcare IT breaches were triggered by vendors whose products contained exploitable flaws.[2] No matter how secure the organization's own policies for cybersecurity are, faulty vendor software products or devices can become the critical point of entry to the organization's system.

In April 2021, the SmartClinic patient information management app from Elekta Inc., was hacked by cybercriminals. This exposed patient identification and health information from the 42 healthcare systems that use the service. The files of these companies were also encrypted and held for ransom.[3]

If healthcare providers don't follow established best practices for vendor management and product/service IT due diligence, such as those published by the National Institute of Standards and Technology,[4] they may be next.

Hazard 2: Inadequate Staff Training

In nearly every industry, including healthcare services, employee error proves to be a critical weak link that allows for cyber infiltration. When employees click links or open documents within a phishing email, they can grant cybercriminals access to the user's account and ultimately to the organization's entire system.

Once they've infiltrated the system, cybercriminals can also begin a new round of internal and external phishing by taking over a user's account and sending seemingly legitimate emails asking for additional confidential information.

Cyber criminals are experts at social engineering,[5] the art of subtly leading an employee to divulge sensitive information or take other dangerous steps they would never make if they stopped to think twice about that action. These kinds of attempts and attacks will continue, and this valuable personal identification information will be vulnerable as long as healthcare organizations fail to continually train employees about cyber risks and what to look out for with both kinds of phishing emails. Some organizations go so far as to periodically send test "phishing" emails to their staff to evaluate vulnerability and provide training moments.

Hazard 3: Not Keeping Cybersecurity Top of Mind

There are many imperatives when managing a successful healthcare facility. Obviously patient and resident care should be job #1. But not far behind, the organization must make cybersecurity an ongoing employee focus with daily reminders about risk scenarios and stories of cyber intrusion in other locations – the errors that were made and the consequences.

Some healthcare systems use an automated caution reminder on emails that come from outside the organization. These can increase vigilance about embedded links, for example, but employees quickly get accustomed to seeing these reminders and their impact fades.

Healthcare employees should be made acutely aware that cybersecurity is a critical new norm, to the point that care providers are also in the business of patient data protection. To have the most impact, these messages must come from the very top, not delegated to the assigned IT security staffer. And these leaders must completely understand the issues and speak the language of cybersecurity so they can credibly communicate that message.

Hazard 4: Failure to Have an Adequately Funded, Ongoing Cybersecurity Program in Place

Defeating cybercriminals means staying one step ahead of them with technology and safe practices. The state of the art is continually advancing, and organizations need to move right along with it. Healthcare IT security team should be encouraged and empowered to explore best practices through industry organizations and other business groups.

Another element of this ideal cybersecurity program is "active threat hunting," in which the organization retains a trusted cyber professional to act as a hacker. This expert explores the organization's IT structure and attempts to uncover security gaps and vulnerabilities.

Still another important aspect of this program is maintaining contingency plans for how to address a cyber intrusion and isolate/limit its impact. These protocols can help minimize the damage if they're promptly adhered to.

Hazard 5: Neglecting to Set and Enforce File Sharing Policies

For reasons suggested above, certain information should never be shared in external and even internal emails and email attachments. If healthcare providers don't establish patient communication portals and insist on their use, the information will continue to be vulnerable. It's important to explain to patients why the organization is using these processes and to emphasize the potential harm and exposure each party could face from cybercriminals if they don't follow these security policies.

Similarly, internal policies should prohibit colleagues from sharing certain patient and client information in electronic communication whenever possible. With those policies in place, employees will ideally think twice when they're asked to respond to a seemingly legitimate inquiry from a co-worker – an inquiry that was spoofed or otherwise socially engineered.

[1] https://www.cdw.com/content/cdw/en/articles/security/the-cost-of-cybersecurity-in-healthcare.html
[2] https://www.scmagazine.com/news/breach/vendor-incidents-lead-the-10-biggest-health-care-data-breaches-of-2021-so-far
[3] https://www.hipaajournal.com/advocate-aurora-health-jefferson-health-and-intermountain-healthcare-affected-by-elekta-ransomware-attack/
[4] https://csrc.nist.gov/publications/detail/nistir/8276/final
[5] https://www.exabeam.com/information-security/social-engineering/

This material is for general information only and should not be considered as a substitute for legal, medical, tax and/or actuarial advice. Contact the appropriate professional counsel for such matters. These materials are not exhaustive and are subject to possible changes in applicable laws, rules, and regulations and their interpretations.
NPN 1316541 | IMA, Inc dba IMA Insurance Services | California Lic #0H64724