Healthcare
INBRIEF®

A Risk Management Bulletin for Allied Healthcare Facilities | 2023 Issue 1

Cybersecurity: Protect Patients by Preventing Data Breaches

A cybersecurity breach in an outpatient setting can seriously compromise patient privacy and safety, as the following examples demonstrate:

- **A hacker breaks into an ambulatory care center's electronic healthcare record (EHR) system,** exposing patient protected health information (PHI), including detailed notes about past illnesses and treatments.
- **A "phishing" attack occurs in an outpatient clinic** when an employee activates a malicious link in an external email, corrupting data from mobile apps and wearable devices and adversely affecting the clinic's diagnostic capabilities. (See "Beware: Phishing Takes Multiple Forms" on page 2.)
- **Due to inadequate security measures, an IT vendor sustains a cyberattack involving ransom malware,** which, in turn, leads to disclosure of clinical data belonging to its client, a diagnostic imaging center.
- **A medical practice administrator loses a laptop computer** containing a large quantity of identifiable patient billing and insurance information.

Such malicious attacks and cybersecurity lapses involving patient databases, email accounts, vendor systems and other elements of an organization's IT infrastructure can have devastating reputational and financial consequences for technology-dependent healthcare settings. In fact, between 2021 and 2022, the worldwide average cost of a healthcare-related data breach exceeded $10 million, more than double the mean per-breach loss for all industries.

To help facilities and practices reduce their cyber exposure, this edition of *inBrief*® reviews vulnerable types of data systems, examines common sources of cyber threats, and suggests practical security measures designed to combat potential attacks by hackers and malware.

Vulnerable Systems

The first step in strengthening IT security requires identifying the areas of greatest vulnerability. According to the Healthcare Information and Management Systems Society, the following systems are especially vulnerable to cyberattacks:

- **Clinical support tools,** including systems relating to documentation, practice management, clinical decision-making, radiology interpretation, computerized physician order entry, e-prescribing and other functions.
- **Medical technology,** including, but not limited to, life support equipment, infusion pumps, blood gas analyzers and remote patient monitoring devices, as well as X-ray machines and other imaging tools.
- **Legacy systems,** such as medical device software and clinical support applications that have been deemed obsolete and are no longer supported by the manufacturer.
- **Vendor programs** that connect third parties to the IT infrastructure of a healthcare facility. (For tips on preventing "crossover attacks" launched from a vendor's compromised system, see "Stopping Crossover Attacks: Vendor Cybersecurity Principles" on page 4.)
- **Email messages that include PHI** and other types of sensitive data, such as financial records or proprietary technology.

Numerous resources are available to help healthcare facilities identify system vulnerabilities and account for how PHI and other critical data are used, stored and secured within the setting. Government-issued assessment tools include the following, among others:

- Cyber Security Evaluation Tool (CSET®), developed by the U.S. Department of Homeland Security.
- Cybersecurity Framework, issued by the National Institute of Standards and Technology.
- Security Risk Assessment Tool, available from the Office of the National Coordinator for Health Information Technology.

By engaging the services of a third-party cybersecurity expert, leaders can help ensure that the tools and techniques they select may be adapted to the organization's needs and IT network.

Common Threats

Cybercriminals may gain access to a computer, portable device or network server in a number of ways, including, but not limited to, the following:

- **Pilfering a flash drive** or other removable media.
- **Finding unsecured laptops** or other devices containing confidential information.
- **Decoding encrypted data** utilizing trial and error methods.
- **Using system privileges** in an unauthorized or illicit manner.
- **Launching phishing attacks** via deceptive emails, as described below.

Beware: Phishing Takes Multiple Forms

While phishing attacks typically occur through personal emails, they also may be launched through websites, social media platforms and text messages. These attacks are often characterized by poor spelling and grammar, as well as an urgent, high-pressure tone. Staff should be trained to guard against the following phishing techniques:

- **"Spear-phishing" emails,** which are sent to a specific employee or department and tend to have a higher "click rate" than generic phishing attempts.
- **"Whaling" emails,** which typically target persons of high rank and seek to deceive the recipient into disclosing organizational and/or financial information.
- **"SMS" phishing,** which occurs when a cybercriminal crafts a deceptive message to a recipient via a text message sent to a mobile phone.

For healthcare-related examples of phishing, see "How To Construct Phishing Campaigns for Various Healthcare Roles." Posted on *infosecinstitute.com*, January 11, 2017.

Phishing email messages illicitly extract sensitive or proprietary information by manipulating recipients into clicking on a malicious link or opening a corrupt attachment. By raising awareness among staff members and providers, unannounced anti-phishing exercises can help limit organizational vulnerability to this type of cyberattack. (For a closer look at phishing techniques, see the box to the left.)

Once hackers have entered an IT system, they may then introduce damaging software, including the following two common varieties:

Malware is a malicious code or software program inserted into a system in order to compromise the confidentiality, integrity and/or availability of data. This threat can take the form of *credential stealers*, whereby usernames and passwords are stolen, or *wipers*, in which entire disk drives are erased. To reduce this risk, the National Institute of Standards and Technology's "Guide to Malware Incident Prevention and Handling" suggests adopting the following preventive measures, among others:

- **Scanning all email attachments** and saving the files to local drives or removable media.
- **Limiting use of removable media** on systems that contain sensitive data.
- **Prohibiting certain types of attachments from being sent or received via email,** such as files with the suffix ".exe."
- **Regularly updating operating systems** and security patches.

After entering a computer or network server, **ransomware** subjects system data to so-called "public-key" encryption involving two keys, only one of which is publicly available. Reading encrypted files requires a second, non-public key, which is provided to the target of the attack only after a ransom is paid. As ransomware programs and methods evolve at a rapid rate, staff and providers should be required to complete information security training sessions upon hire, and at a minimum, annually thereafter. These classes should describe the risks of improper data disclosure, present basic cybersecurity measures and offer guidelines for the handling of sensitive patient data.

In addition, staff should be informed of the potential consequences of hazardous data management practices, such as removing PHI from the facility, sharing passwords, exposing laptops or storage devices to theft, and leaving confidential information displayed on the screen. These cybersecurity training and educational measures should be buttressed by sound incident response and business continuity plans that may be deployed in the event of a ransomware attack.

Security Measures

Policy development. Sound, consistently enforced cybersecurity policies represent an essential first step in minimizing risk. Protocols should address data access restrictions, staff and provider conduct expectations, incident response measures and other critical security-related issues.

Anti-virus software. These vital tools are used both to detect viruses in incoming emails and prevent "infections" from spreading throughout the IT system. Coupled with endpoint detection and response (EDR) technology – which facilitates the monitoring of end-user devices such as mobile phones, laptops and medical devices – anti-virus programs can help administrators monitor data flow, detect irregularities and respond to patterns of malicious activity.

User authentication and monitoring. Common user verification methods include passwords, security codes and biometric tools. To optimize security, ensure that user accounts include routinely reset passwords, lock automatically after a set number of unsuccessful login attempts and log user access to protected information, in accordance with the HIPAA Security Rule.

Data encryption. Password protection alone is insufficient to ensure data privacy. Confidential data should be encrypted and readable only to those with the associated electronic key.

Device regulation. A formal medical device management system – including an inventory to identify outdated and no-longer-supported devices – can help enhance cybersecurity. (For additional recommendations, see "Medical Device Cybersecurity: What You Need to Know," issued by the U.S. Food and Drug Administration.)

Business continuity. Healthcare facilities must implement a plan to maintain operations in the event of a cyberattack. The business continuity plan should address such issues as technical redundancy, EHR downtime protocols (including manual alternatives) and specific recovery objectives, including time frames. The plan also should include contact information for hardware and software support vendors.

Incident response. A comprehensive incident response plan can help significantly mitigate damages following a cybersecurity incident. The plan should include the following steps, among others:

- **Determine the severity, scope and root causes of the data breach,** retaining forensic experts, if necessary.
- **Notify potentially affected patients.** In general, it is advisable to inform all affected parties of a data breach, even if such notification is not legally mandated.
- **Offer credit and medical identity monitoring services to affected individuals,** following consultation with legal counsel.

Cyber liability coverage. Specialized cyber insurance products exist to address data- and privacy-related exposures. These policies typically cover third-party liability, as well as notification costs, system restoration expenses and business interruption losses consequent to a data breach.

Every healthcare facility must be vigilant in guarding against data breaches and system infiltrations, which can endanger both patient confidentiality and safety. By understanding the nature of the threat and implementing appropriate countermeasures, healthcare leaders can help turn this potentially catastrophic exposure into a manageable risk.

A comprehensive **incident response plan** can help significantly **mitigate damages** following a **cybersecurity incident**.

Quick Links

- Cybersecurity, a resource page of the National Institute of Standards and Technology.
- Pino, L. "Improving the Cybersecurity Posture of Healthcare in 2022." Posted February 28, 2022 on the website of the U.S. Department of Health & Human Services.

Stopping Crossover Attacks: Vendor Cybersecurity Principles

Many cybercrimes involve so-called "crossover" attacks in which computer networks are infiltrated through third-party vendors. For this reason, healthcare organizations should implement a proactive vendor cybersecurity program that includes the following strategies, among others:

- **Perform cyber risk assessments of prospective vendors,** focusing on such key issues as the scope of the company's internal compliance standards and the effectiveness of its safeguards.
- **Identify vendors with frequent network access** and discuss cybersecurity concerns with them, seeking mutually beneficial methods to reduce vulnerability to hackers.
- **Conduct regular security checks** in the form of questionnaires and/or in-person assessments. In particular, look for use of unpatched software and failure to scan incoming data for the presence of malicious code, as well as points where vendors connect to the IT infrastructure using outdated laptops, tablets or computers.
- **Examine service agreements regarding data sharing and security,** especially in view of the HIPAA Privacy Rule's "minimum necessary" standard.
- **Ensure that contracts with vendors expressly address PHI confidentiality issues** in accordance with federal and state statutory and regulatory guidelines.
- **Require that all contract language – including indemnification and hold harmless agreements – be reviewed** and approved by legal counsel and IT specialists.
- **Partner with an expert cybersecurity team** to evaluate vendor compliance and issue monthly or quarterly reports.

Did someone forward this newsletter to you? If you would like to receive future issues of *inBrief*® by email, please register for a complimentary subscription at go.cna.com/HCsubscribe.

For more information, please call us at 866-262-0540 or visit www.cna.com/healthcare.