Where to Begin with Cyber Defense

Save to myBoK

By Sharon Lewis, MBA, RHIA, CHPS, CPHQ, FAHIMA, and Kevin B. McDonald, HCISPP, CHPSE

As data is made more readily available through a growing number of public and private channels, understanding the risks is critical. Patients expect organizations to take the steps required to protect their sensitive and personal information as it is being produced, processed, shared, and possessed. Whether it is protected health information (PHI) or personally identifiable information (PII), health information management (HIM) professionals have an ethical and legal obligation to protect patient data from wrongful use and disclosure. This of course is not an easy feat, and this article is designed to provide advice for those parties intent on meeting their breach prevention obligations to patients and the federal government. According to the Ponemon Institute's "Fourth Annual Benchmark Study on Patient Privacy & Data Security," criminal attacks on healthcare have risen 100 percent since the study was conducted four years ago in 2010. In April and August 2014, the Federal Bureau of Investigation (FBI) issued a notice warning that healthcare systems and medical devices face an increased risk of cyberattacks and hacking.

The demand for patient information remains high on criminal marketplaces, including the 2014 release of Grams, a search engine for what is known as the Dark Web. The Dark Web loosely refers to many websites that are publicly available, but whose ownership is obscured by several methods to protect those responsible for their management. With Grams, criminals are removing the knowledge barrier to obtain illicit information, products, and services. The newly minted search engine aids those seeking underground or illegal products and information such as stolen PHI and PII, drugs, guns, heavy artillery, prostitution, and the services of mercenaries. There is even a YouTube video demonstration on how to use Grams.

If you are looking for one good example of a bad data breach, look no further than the recent incident involving Community Health Systems, Inc. According to the company's Securities and Exchange Commission 8K filings, the cyber attack that occurred in April and June 2014 impacted "data related to the company's physician practice operations and affected approximately 4.5 million individuals who, in the last five years, were referred for or received services from physicians affiliated with the company," the filings state.

Many have asked who the attacker was in this security breach. The company and its service provider "believe the attacker was an advanced persistent threat group originating from China who used highly sophisticated malware and technology to attack the company's systems. The attacker was able to bypass the company's security measures and successfully copy and transfer certain data outside the company," the filings state.

Healthcare Should Brace for More Cyber Attacks

In a recent warning, the FBI said "Cyber actors will likely increase cyber intrusions against health care systems—to include medical devices—due to mandatory transition from paper to electronic health records, lax cybersecurity standards and a higher financial payout for medical records in the black market."

In an attack, criminal cyber actors may seek information such as credit card numbers, medical record numbers, a patient's diagnosis, and other health data that can be used to, among other things, steal a patient's identity, access individuals' bank accounts, and obtain prescriptions for medications. It is well understood that patients' medical information is worth around 10 times more than credit card numbers on the black market, as reported by *Reuters*. In addition to the higher record value, victims of healthcare identity theft usually take longer to report an incident and recovery can be extremely difficult. It often may take weeks or months to realize that information has been taken, and it can take years to recover.

Medical identity theft is difficult to recognize. For HIM professionals concerned with patient privacy, being aware of these attacks is key to prevention. Understanding which safeguards need to be in place to ensure confidentiality, availability, and integrity of the PHI and PII is also vital to successful cyber defense. The need to protect patients' information includes at least basic knowledge of the types of cyber-crime occurring in today's environment and how they come about. Understanding how these events may occur and ensuring mitigation strategies are in place can significantly decrease the risk of PHI and PII compromise. Keep in mind, even when a breach does not immediately cause tangible damage to the patient, the damage to a provider's reputation—along with financial liability—can still be significant.

Common Ways Systems are Attacked

Cyber breaches may occur in a variety of different ways. Whether it is insiders making mistakes or intentionally releasing information, hackers directly targeting an organization, or random broadcast scanning that simply attacks many targets, the cyber breach possibilities can be overwhelming. Identity theft, for example, may be due to employees stealing information such as pharmaceutical and prescription data and selling it. Some common attacks and breach causes include:

Viruses, worms, trojans, and bots. These programs, also known as malware or malicious code, are specifically designed to damage, disrupt, steal, or inflict some "bad" or illegitimate action on data, host computers, or networks.

Theft or loss of data bearing devices. Cell phones, CDs, DVDs, thumb drives, and laptops are among many other devices that pose a large threat to organizations. According to Ponemon, 36 percent of reported breaches are due to a lost or stolen laptop.

SQL injection. A coded statement inserted into an entry field designed to dump database contents to an attacker.

Phishing. A targeted individual is contacted by e-mail or telephone by someone posing as a legitimate institution to lure an individual into providing sensitive information such as banking, credit card details, and passwords. This can be done by suspicious links in e-mail or false advertising, among other methods.

Web-based attacks. Malware and social engineering attacks that target end users and web-connected devices by displaying bogus pop-up windows made to look like legitimate plug-ins that prompt a user to click on it and open the gate to infect a computer device.

Social engineering. An act of psychological manipulation that targets human decision making. For example, an individual walks into a building and posts an official looking announcement stating the help desk number has changed. When an employee calls for help, the individual might ask for a password and ID to obtain access to the company's private information.

Misconfigured systems. This can be identified as a main cause of a breach and may consist of unsecured wireless access points, mismatched applications and hardware, and security systems not regularly maintained. These networks can be easily penetrated by hackers.

PHI protection requires that an organization implement administrative, physical, and technical safeguards to protect the privacy, availability, and integrity of their data. HIM professionals help facilitate PHI protection by being clear on where PHI resides within all systems in the organization and by completing an entity-wide risk assessment of all identified systems, processes, and facilities. Also, a policy should be implemented that prevents non-technical users from having administrative rights and ensures administrator accounts are only used for functions that require such access.

Utilize anti-virus and malware protection software and keep the signatures up-to-date, and ensure that all systems are patched and updated to help close vulnerabilities that are leveraged by bad actors, viruses, and other malware. Ensure that the organization's network is protected by firewalls with advanced threat protection. Also, use unique and complex passwords and ensure they are changed on a regular schedule, preferably every 90 days. Organizations should implement encryption for data in transmission and at rest, and identify the internal and remote access points where a connection may exist with other systems that contain PHI in order to make sure they are secure. Create procedures to authorize and control workforce access to PHI, audit systems access and maintain documentation of those audits, and document, implement, and enforce policies and procedures through employee education and sanctions policies. HIM professionals should also implement security monitoring and log review processes, as well as implement a media inventory management program while documenting all changes to their system.

Surrender is Not an Option

While this may seem like a lot to handle, surrender is not an option. IT security is about risk management and ensuring that an organization has an ongoing risk management program. Being proactive means conducting a comprehensive and ongoing security risk analysis. If critical threats are identified and resolved first, before an attack, and systems are maintained by continually working to reduce the quantity and severity of risk, organizations stand a better chance against the ever-changing threat landscape.

Resource

Ponemon Institute. “Fourth Annual Benchmark Study on Patient Privacy and Data Security.” March 12, 2014. www.ponemon.org/blog/fourth-annual-benchmark-study-on-patient-privacy-and-data-security.

Sharon Lewis (slewis@primeauconsultinggroup.com) is principal and chief privacy officer for Primeau Consulting Group. Kevin McDonald (kmcdonald@noloki.com) is chairman of the Orange County Sheriff/Coroner’s technology advisory council and president of Noloki Healthcare IT and Compliance.

Article citation:
Lewis, Sharon; McDonald, Kevin B. "Where to Begin with Cyber Defense" *Journal of AHIMA* 86, no.4 (April 2015): 40-41.