CHAN Healthcare™

A subsidiary of Crowe Horwath LLP

Emerging Issue

Data Security

In August 2014, Community Health Systems Inc. disclosed that its computer network was a target of a hacking incident resulting in the exposure of information – names, telephone numbers, Social Security numbers, addresses, and birthdays – for approximately 4.5 million patients. It was the second-largest breach of patient information in history. Although the monetary impact of the breach is yet to be determined, Forbes estimates the cost to be upward of $75 million once monetary penalties, legal fees, and theft protection and credit monitoring for affected patients are taken into account.

In September 2014, additional hacking incidents were reported, including a breach at HealthCare.gov, the federal government website where Americans sign up for healthcare plans through the *Affordable Care Act*. Although that incident did not compromise customer information, the attack crashed servers, and users were unable to access the website.

The number of data security incidents resulting from hacking, malware, and theft continues to rise each year. According to Symantec Corp.'s 2014 Internet Security Threat Report, information breaches increased globally by 62 percent in 2013. More than 552 million identities were exposed via breaches in 2013, 38 percent of mobile-device users experienced a mobile-device cybercrime in the past 12 months, and 1 in 392 emails contain a phishing attack.

Hackers often start by collecting information about the intended target and then identify potential methods of attack. Four types of attacks are typical, and potential controls exist for each type:

1. **Logical security attack:** Attempting to break passwords or exploit unchanged system default passwords. (Potential controls include strong password settings, system monitoring, and audit logs.)
2. **Physical security attack:** Attempting to break into a physical location such as a data center, office, or network closet. (Potential controls include door locks, motion detectors, and camera systems.)
3. **Network attack:** Attempting to break into an organization's network perimeter to exploit internal network vulnerabilities. (Potential controls include firewalls, intrusion detection systems, and security patches.)
4. **Social engineering attack:** Attempting to gain access to sensitive information through a user. (Potential controls include security awareness training, spam filters, and anti-virus software.)

This list of potential controls is not exhaustive. Healthcare organizations should perform a risk analysis and implement appropriate controls to prevent, detect, and respond to an attack.

SUMMARY

Through the federally mandated push for electronic health record systems and health information exchanges, healthcare organizations are moving toward system integration. The increased use of healthcare technology, coupled with rising data security risks, heightens the risk of exposure of electronic protected health information (ePHI).

Contact Information

Raj Chaudhary, CGEIT, CRISC
312.899.7008
raj.chaudhary@crowehorwath.com