HOW HOSPITALS CAN IMMUNIZE AGAINST HACKERS

by Jared Rhoads, Richard Staynings and Ashif Jiwani

Cybercrime and data breaches are among the most commonly cited worries keeping healthcare CIOs awake at night. Recent surveys show that roughly three-quarters of healthcare organizations have suffered some kind of data breach or security incident in the past 12 months.

Hospitals and other healthcare organizations need to broaden their focus on compliance and pursue a robust, integrated, enterprise-type approach to securing data and other key assets.

Under the U.S. Health Information Technology for Economic and Clinical Health Act, hospitals and other organizations can be fined up to $1.5 million per year for serious security incidents.

Recently, the Department of Health and Human Services' Office for Civil Rights issued for the first time a financial penalty for a *non-major* breach (i.e., a breach affecting fewer than 500 individuals). In this instance, a hospice company in Idaho that reported the theft of a laptop will be required to pay a $50,000 fine and agree to a corrective action plan. The incident is believed to have affected 441 individuals.

The full cost of a breach, however, goes far beyond the fines. According to Ponemon Institute, the cost of identifying and notifying affected individuals — now mandatory under the law — is on average $214 per record. There are also intangible costs associated with compromised trust and reputation, as well as other significant costs, including harm to health, or even death.

Cybercrime is well-organized, and cybercriminals will go after valuable information wherever it resides, including within healthcare organizations. Typically, cybercriminals do not distinguish based on public versus private sector, type of institution or other such factors. Instead, they target the most valuable information and sell it to the highest bidder. According to the World Privacy Forum, a stolen medical identity has a street value of $50 today, compared to $14 – $18 for a credit card number or $1 for a Social Security number.

Most hackers who infiltrate health IT systems are seeking financial data, not medical information. In an analysis of 855 data breaches involving more than 174 million records from the healthcare, financial services, retail and hospitality industries, researchers found that such breaches are "almost entirely the work of financially motivated organized criminal groups, which typically attack smaller, low-risk targets to obtain personal and payment data for various fraud schemes," according to a Verizon Communications 2012 Data Breach Investigations Report.

BYOD presents new weaknesses

Cybercriminals constantly target new areas of perceived weakness. Three of the newest trouble areas for healthcare organizations are mobile devices, portable media and medical devices.

Mobile devices are targeted by cybercriminals interested primarily in identity and financial theft. Although most breaches still come from laptops and paper records, breaches related to mobile devices are rising the fastest. According to a recent CSC survey of IT executives, 57% of respondents named mobile clients and unmanaged devices their top security challenge.

Resisting the bring-your-own-device (BYOD) movement, however, is not the best solution. Rather, organizations should design a secure way to allow employees to use their own equipment to do their work without increasing risk to the organization.

Portable media is another prime target, especially for cybercriminals interested in identity theft, insurance fraud and financial theft. Loss and theft of portable media have affected more individuals than any other type of breach. Besides setting and enforcing clear policies and procedures surrounding the use of portable media, it is important to employ technical safeguards as well.

Medical devices also need protection. These devices are a new target of choice for cybercriminals out to wreak havoc by causing equipment failures and malfunctions. To date, no medical injuries in the United States have been reported as a result of infected medical devices, but sophisticated malware has been "running rampant," according to some government officials and hospital IT staff.

Gaining cyberconfidence

With lives at stake, security must involve more than locking down individual applications and systems; today's threats require a holistic approach. Achieving cyberconfidence enables organizations to engage securely with patients, partners and others in a context of mutual trust. It is the knowledge that the organization can react to any threat or incident with speed and agility.

One step toward cyberconfidence is performing a comprehensive risk assessment. An organization can undertake its own risk assessment or enlist the help of outside experts. Publicly available tools also can help.

Once healthcare organizations complete a comprehensive risk analysis, security should be made part of an ongoing process of improvement that ties together security, compliance, risk management and corporate governance.

As security threats grow more complex and challenging to keep up with, many organizations are turning to managed security service providers for 24-hour network monitoring, incident tracking and immediate incident response. This level of detection and response is critical to an organization's security.

A recent review of healthcare data breaches found that nearly two-thirds persisted for months before they were detected, giving criminals ample time to do damage.

Staying current with cyberthreats can be challenging, but IT security should not hinder an organization's growth or prevent it from using data assets to improve care delivery, quality and financial performance. With increased vigilance and the right technological tools, healthcare organizations can achieve true confidence in their cybersecurity. ■

JARED RHOADS is a senior research specialist with CSC's Global Institute for Emerging Healthcare Practices.
RICHARD STAYNINGS is a CSC cybersecurity and privacy officer.
ASHIF JIWANI is a partner with CSC's Healthcare Group.

5 WAYS TO PROTECT HEALTHCARE DATA

Regardless of your current risk profile, consider these ideas and recommendations at your next high-level security meeting:

1. Deploy advanced network monitoring. Organizations need automated tools to assess vulnerabilities and look for breaches. Seek out advanced tools to self-test the effectiveness of your firewall and consider egress solutions, which automatically monitor what is being sent outside the walls of an organization, where it is being sent and when.

2. Develop a 21st-century strategy for mobile devices and medical devices. You cannot fight the bring-your-own-device movement, but you can manage it and help employees make good decisions. Embrace security practices that are easy for end users. Try integrating part of the IT security function with the biomedical engineering services department.

3. Make system authentication multifactor and adaptive. Multifactor authentication systems are much preferred over systems that use only passwords. Multifactor systems are expensive and take a long time to deploy, so get a head start before they become required.

4. Test yourself by contracting with ethical hackers. Using ethical hackers to try to find exploits from the outside can help to identify more obscure vulnerabilities that may have been overlooked. Ask ethical hackers to test your technical environment as well as the training of your staff (i.e., through social engineering).

5. Consider whether purchasing cyberinsurance might be right for you. New insurance products on the market are designed specifically with hospitals and other healthcare organizations in mind. While insurance won't make your systems more secure, it can help you feel more confident about your ability to survive a major adverse incident.

Learn more at
csc.com/health_services.