HEALTHCARE IT
DIGITAL COMMUNITY

HIMSS: EHR, mobile device use catapult security threats

February 23, 2012
By: Cynthia Keen

LAS VEGAS - Do you use mobile tablets and smartphones as extensions of your radiology information system and PACS? Do you use them to access hospitals' electronic health records (EHRs)? Do they have traces of protected health information (PHI) when you turn them off? Do you even know what PHI is?

Mobile devices have become a part of imaging informatics delivery hardware, and because of this, they need to be part of the security plan of a radiology practice, imaging center, and radiology department. If you answered "yes" to either the first or second question posed above, and anything but "no" to the third, then a presentation made at the Healthcare Information and Management Systems Society (HIMSS) annual meeting on Wednesday about security breaches in healthcare should be of great interest to you.

In just three years, the number of healthcare data breaches in the U.S. has skyrocketed, putting the healthcare industry at the top of all industries monitored for security violations, according to the 2011 Threat Report from data protection and security firm Symantec. In 2009, its ranking had been 15th.

What is causing this? Healthcare security specialists Mac McMillan, president of healthcare security firm CynergisTek, and Adam Greene, an attorney at Davis Wright Tremaine who counsels healthcare organizations on compliance with HIPAA privacy, security, and breach notification requirements, blame ignorance, complacency, an "it won't happen to me" attitude, and an inadequate amount of human and financial resources expended.

In spite of HIPAA requirements to protect patient data that went into effect in 2003, and the steady conversion from paper-based to electronic data exchange and recording of patient information, most healthcare organizations and physician practices have spent far less than other industries on security measures. During 2011, 70% of respondents to an annual security survey conducted by HIMSS Analytics reported that their organizations spent 3% or less of their annual healthcare IT budget on security. The average for all industries in 2011 was 6%, McMillan told *AuntMinnie.com*. This was the fourth consecutive year that healthcare organizations reported they spent less than the industry average.

Medical specialties such as radiology are not exempt. Based on CynergisTek's consulting engagements, radiology departments, imaging centers, and the offices of radiology practices are among the least protected and least knowledgeable about security measures they should routinely be undertaking, McMillan said.

Sobering statistics

Data breaches affecting 500 or more patients rose by 32% in 2011. Between 2009, when reporting breaches to the U.S. Department of Health and Human Services (HHS) became mandatory, and October 2011, data on more than 18 million patients were compromised in 380 incidents. During this time, more than 30,000 breaches affecting fewer than 500 patients were reported, Greene said.

Interestingly, the number of breaches has remained relatively constant, averaging 18 major breaches a month. The rise in use of mobile devices has contributed to breach incidents, but it's not the only problem. Nor is malicious hacking, although healthcare is now included as a subject in hacker conferences such as Def Con and Black Hat.

The biggest problem is theft (52% of the total number of breaches) and loss (14%) of desktop and laptop computers, portable electronic devices including mobile tablets, storage devices such as flash drives, and smartphones. Unauthorized access represents 20% and improper disposal of medical records represents 5%. Hacking is attributed to 7%.

While the largest number of breaches of any type are paper-based (26% of the total), they only involve 3% of the more than 18 million affected patients. "You've got to steal records by the truckloads to get a high volume, but a single thumb drive can contain thousands of records. If you want to have a breach on a really huge scale, there is no substitute for electronic information. It has totally changed the nature of the threat landscape for the healthcare industry," Greene commented.

What to do?

McMillan and Greene are quick to emphasize that theft and loss should not entirely be blamed on thieves outside the healthcare organization. An unsettling number of breaches are attributed to thefts of portable electronic devices and laptops from cars, public transportation, desks, briefcases, and purses of employees and physicians in transit.

Be concerned about your workforce, they advised. People forget to lock rooms where servers and backup tapes are stored. They forget to lock their desks.

Also, encrypt everything. Green pointed out that according to a well-respected security industry survey, only 60% of respondents in the healthcare industry reported encrypting mobile devices. Only 50% of backup tapes, 45% of any type of media, and 35% of servers and databases were encrypted.

Regularly conduct a thorough risk assessment and analysis of security measures, they recommended. Security is dynamic, and threats change over time, along with people, equipment, and software systems. When performing due diligence, engage an objective third party and adopt industry recognized IT security models. A number of models exist for healthcare organizations that can serve as benchmarks to measure compliance.

Finally, develop a detailed remediation roadmap and a project plan to guide decisions, and provide IT staff with the training, tools, and resources to implement and maintain a robust security program.

Security practices of associates and vendors

The most robust internal security program won't protect a healthcare organization from breaches caused by business associates. From 2009 through October 2011, only 22% of large breaches reported to HHS were caused by business associates, but these represented 62% of affected patients.

"We are seeing a trend of the largest breaches being caused by trusted partners," Greene said. "The aftermath can be devastating."

He referenced the multimillion dollar lawsuits filed against Science Applications International (SAIC), an EHR contractor for military healthcare provider Tricare, both of which are being sued for up to $4.9 billion in class action lawsuits. Backup tapes containing records of 4.9 million retired military personnel and their families were lost in what has been attributed to a car theft as they were being transported from one facility to another in September 2011.

Stanford University Hospital has also found itself in the national media limelight. Names, diagnostic codes, and billing amounts for approximately 20,000 patients treated in its emergency department between March and August 2009 had been posted on a public website, Student of Fortune, for almost a year before being discovered. The homework help website had posted the information so that it could be used to show students how to create bar graphs.

How did the site get these data? The file was created by a subcontractor of one of the hospital's business associates, Multi-Specialty Collection Services.

The lesson to be learned is that healthcare organizations need to reduce risk when they give data to business associates by evaluating the security practices of business advisors, and by including security requirements in contracts. Perform due diligence, but allot time and resources -- including third-party reviews and audits -- according to which business associates will have access to the largest amount of data, McMillan and Greene suggested. However, as in the case of SAIC, this is still no guarantee that data will be safe even in the hands of the most security-astute business advisors.

Healthcare organizations should also develop a vendor management security strategy, according to McMillan and Greene. Communicate your expectations with respect to data security. Who has access to data? Why? What are these individuals permitted to receive? How do they protect it on their site? How do they transmit data back and forth? When a contract terminates, how is data going to be disposed of? Security requirements should be clearly spelled out in the terms of a contract. This is especially applicable for RIS, PACS, and offsite archive vendors.

What about radiologists? And what is PHI?

Radiology IT departments have often functioned as a separate entity from a hospital's IT department, although this trend is changing. The security guidelines that exist for a hospital may not be applied in a radiology department, McMillan said, which could result in the hospital's RIS and PACS being less secure than they should be. An often overlooked vulnerability in radiology departments is when other RIS and PACS can be accessed outside the hospital, and the security protection of these systems might be unknown, he also noted.

The need to protect imaging equipment is also sometimes overlooked. McMillan said that some recent hacker conferences he attended included discussions on how to hack a CT, MRI, and/or PET scanner, especially ones that use wireless commands. A hacker can change radiation doses to be delivered, modify protocols, and alter image processing so that the image is incorrect even if an exam was correctly performed. This is not theft of data, but it's security penetration that could seriously affect patient safety.

Radiologists who use smartphones and mobile tablets need to be aware that these may contain traces of PHI even after they have been turned off. For this reason, data need to be encrypted, and all devices need to be password-protected.

"It's important for radiologists to understand the value of their information," Green said. " ‘Who wants a digital x-ray?,' a radiologist may ask. This is a dangerous mindset to have."

Rather, Greene and McMillan recommend that radiology practices think of the repercussions if patient data are compromised. Any size data breach will cost time, money, and the resources of the practice. There may be multiple lawsuits to deal with, fines from government agencies, and adverse publicity. Patient referrals, revenue, and contracts may be lost.

The costs, time, and resources involved in implementing robust security measures and maintaining them pale by comparison.

http://www.auntminnie.com/index.aspx?sec=sup&sub=ris&pag=dis&ItemID=98428