Healthcare IT News

Healthcare security stuck in Stone Age

New report shows industry is 'behind the curve' with security

Healthcare has a few things to do differently in the privacy and security arena -- one of them being: Start taking it seriously. The new 2014 Verizon Data Breach Investigations Report highlights a concerning carelessness regarding privacy and security, specific to the healthcare industry.

"They seem to be somewhat behind the curve as far as implementing the kinds of controls we see other industries already implemented," said Suzanne Widup, senior analyst on the Verizon RISK team, in an interview with *Healthcare IT News* discussing report findings.

The industry's biggest misstep? Encryption, encryption, encryption.

After examining some 63,000 security episodes and upwards of 1,300 breaches from 50 data-sharing partners, Verizon officials found that the lion's share of data breaches -- 46 percent -- stem from physical theft or loss of unencrypted devices.

This stands as the highest percent across any of the 19 industries analyzed in the report. So, not only are organizations failing to encrypt mobile devices and laptops, but healthcare employees are also being notably negligent with how they handle these devices -- leaving them unsecured in personal residences or personal vehicles, for instance.

"(Physical theft and loss) is the biggest problem in healthcare that we are seeing," said Widup. "It really surprises me that this is still such a big problem. It's one of those things that encryption is such an easy safe harbor," she pointed out. "Other industries seem to have gotten this fairly clearly."

Of course, the healthcare numbers are going to be slightly higher because the federal government has mandated specific HIPAA privacy and security breach notification requirements for organizations, but that doesn't change the reality that these organizations still fail to implement basic encryption practices, added Widup.

The healthcare sector also saw its second highest numbers in the insider misuse category, with 15 percent of healthcare's security incidences due to insider misuse. That's higher than 13 other industries. Only the administrative, mining, public sector, real estate and transportation industries saw bigger numbers.

Widup said they see insider misuse "quite a bit," especially affiliated with organized crime groups where they either have someone recruited as an insider or they are specifically sent to get a job in healthcare where they eventually facilitate access to sensitive information that's easily monetized, like Social Security numbers associated with patient records, for instance.

Tax fraud is also big in this category, Widup pointed out, especially in Florida. "Florida is the leading edge of this kind of attack," she said.

There's also the employee snooping problem, which Widup said is actually underreported, as it doesn't have the financial backing that say tax fraud has.

The most effective method to curb these occurrences is by auditing your users and the data, said Widup. "You need to know who has the data, who has access to the data, and you need to monitor it," she said. "When you see organizations implement some sort of auditing scheme, suddenly they start finding a lot of stuff they couldn't see before."

"When organizations implement some sort of auditing scheme, suddenly they start finding a lot of stuff they couldn't see before."

Healthcare also stands out in the miscellaneous error category, accounting for 12 percent of the industry's security incidences.

This occurs when say, for example, employees send paper documents or emails to the wrong recipient, or publish data they thought was protected but turns out it could be found via a simple Google search.

Case in point is what transpired at the three-hospital Cottage Health System last year when the protected health information of nearly 33,000 of its patients was compromised after patient data was found on Google due to a removal of electronic security protections.

Nashville, Tenn.-based Cogent Healthcare also recently reported a similar incident when a site the hospitalist company was using to store patient data had its firewall down, exposing the protected health information of some 32,000 patients.

These types of cases, Widup pointed out, could most often be avoided by a simple quality sampling process. Try a few envelopes with letters before sending out the entire thing. "These kinds of quality insurance things are basic to a lot of industries, but they don't think about it for things like this," she said.

From Healthcare IT News – April 22, 2014 -
http://www.healthcareitnews.com/news/healthcare-security-stuck-stone-age