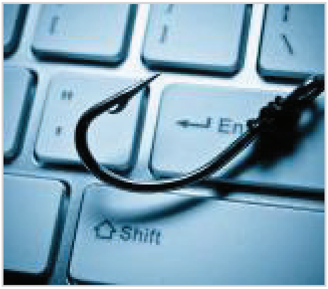
HEALTHCARE INFORMATICS

Published on *Healthcare Informatics Magazine* | *Health IT* | *Information Technology* (http://www.healthcare-informatics.com)

Healthcare Leads Data Breaches in 2015, Human Error Still Leading Cause, Report Says

April 1, 2016 by Heather Landi

| Reprints



Click To View Gallery

Given the recent high-profile ransomware and malware attacks on healthcare organizations, such as Hollywood Presbyterian Medical Center and MedStar Health, it is perhaps not surprising that a recent report found that the healthcare industry saw the highest number of data security incidents in 2015.

Law firm BakerHostetler's 2016 Data Security Incident Response Report, titled "Is Your Organization Compromise Ready?," found that of the 300 data security incidents on which the firm advised in 2015, 23 percent occurred in the healthcare industry, followed by financial services, 18 percent, and education, 15 percent.

However, the good news is that while healthcare companies topped the list of frequency of breach incidents by industry, the report findings show that the healthcare industry incidents are less severe than those that occur in other industries, on average. "While frequency was high, the severity measured by number of potentially affected individuals was relatively low (fewer than 500 individuals per incident on average)," the report authors stated.

Topping the severity list by number of individuals affected was restaurants/hospitality, mostly due to financially motivated attacker groups moving their focus from grocers and big-box retailers to restaurants, hotels, and casinos, the report authors wrote. The average size of notification for restaurants/hospitality was 2.2 million people, according to the report.

According to the report findings, phishing/hacking/malware accounted for 31 percent of data security incidents across all industries in 2015, taking the number one spot from human error, which was the leading cause of incidents in last year's report. In 2015, employee action/mistake accounted for 24 percent of data security incidents. "However, when we looked at the underlying issues that enabled many of the phishing/hacking/malware incidents to succeed, they could often be attributed to human error in some way, so in a way our numbers show that human error is a factor over half of the time," the authors wrote.

Within the healthcare industry, human error, more specifically employee action/mistake, was still the leading cause of security incidents in 2015, accounting for 34 percent of incidences. Phishing/hacker/malware accounted for 15 percent of data security incidents in healthcare, tied with vendors, and then followed by external threat (14 percent), internal threat (12 percent) and lost or improper disposal (10 percent).

Across all industries, the report findings indicate that detection capabilities need to improve. The report also looked the incident response lifecycle—detection, containment, analysis and notification. Analyzing the 300 incidents, on average, it took 69 days from occurrence of the incident to discovery and the median was 15 days. Within the healthcare industry, the average from occurence to detection was 114 days.

The average time from detection until containment was seven days. According to the report, one factor that can make a big difference in speeding up the time from detection to containment is a company's ability to get a forensic firm engaged and then provide the firm with forensic data and visibility into the environment. “Companies that have already identified the firm they will work with, that already have a Master Services Agreement “MSA” in place, and that conducted scenario planning together usually reach containment faster and with less impact to business operations,” the report authors stated.

“Other companies that fared better were ones that had detailed, lengthy, and centralized logging. And companies that used forensic firms with tools that enabled the firm to look quickly for indicators of compromise across many endpoints also often reached containment faster. Those companies for which the findings came from only imaging devices had slower containment.”

An average it took 43 days to complete forensic investigations, and it took 40 days from discovery to notification.

The report also noted that the data at risk that led to the decision to notify in 61 percent of analyzed incidents was data subject to state breach notification laws—generally a person’s name associated with a Social Security number, driver’s license number or financial account information. Health information was affected in 27 percent of the incidents.

“Every company should be constantly focused on preventing, detecting, and having the right capabilities in place to respond to incidents. Accepting that incidents are inevitable does not mean that you stop trying to prevent them. In addition to reducing risk profiles through information governance and implementing preventative security measures, companies must focus on adapting measures to changing risks along with faster detection and containment to effectively respond,” the report authors wrote.

The outlines eight strategies for organizations to be “compromise ready”:

- Employ preventative and detective security capabilities
- Threat information gathering, such as incorporating endpoint monitoring and a SIEM to aggregate logs.
- Personnel awareness and training as there are limits to technology
- Proactive security assessments focusing on identifying the location of a critical asset and data and implementing reasonable safeguards and detection capabilities around them
- Assessing and overseeing vendors
- Developing, updating and practicing incident response plans; conduct tabletop exercises that reflect reality
- Understanding current and emerging regulatory hot buttons
- Evaluating cyber liability insurance

The report authors note that companies can most improve in three areas—detect incidents sooner, contain them faster after detection and keep good logs to facilitate a more precise determination of what occurred before the attack was stopped.

Topics