Swiped, Not Hacked: After a Year of Reporting, Theft Remains Main Cause of Breach

Save to myBoK

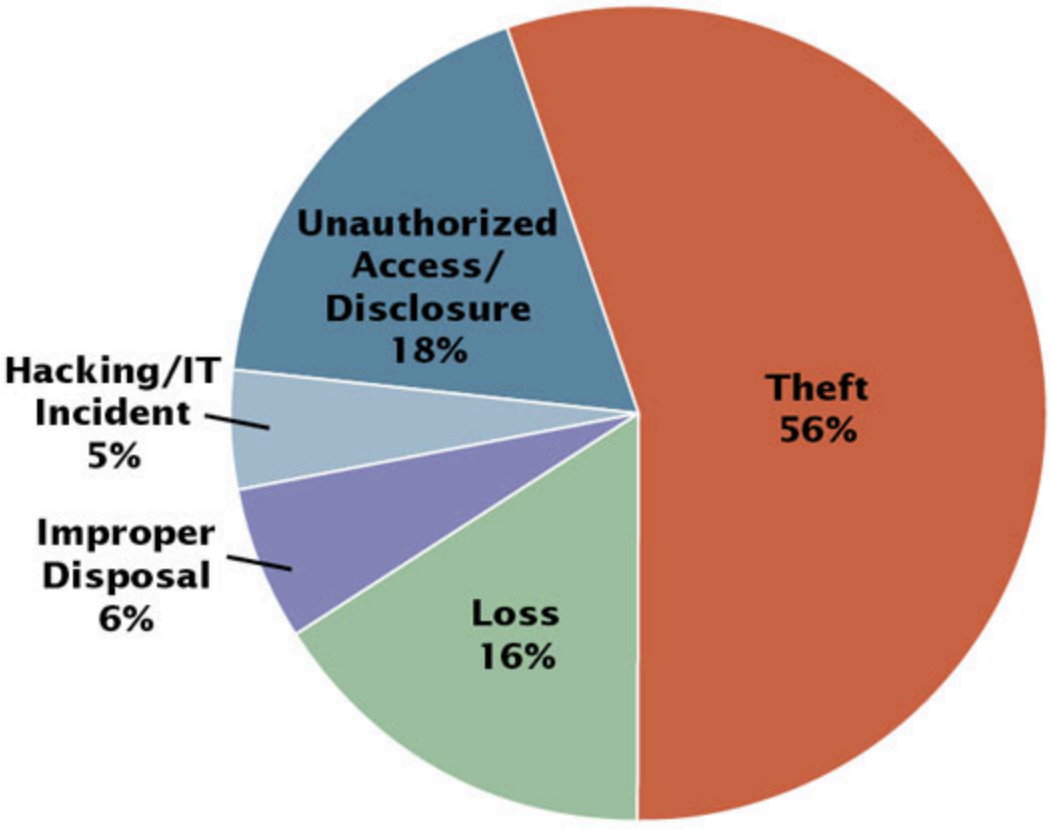
With one year of breach reporting on the books this month, theft remains the most common cause of data breach in healthcare. Of the 217 large-scale breaches reported to the Department of Health and Human Services by mid-January 2011, 121 (56 percent) involved theft. Of those, 89 involved a laptop, desktop, or network server.

Lost equipment or records accounted for an additional 34 breaches. Together, loss and theft account for more than seven in 10 of the breaches on file, involving unsecured, personal information on more than 5 million people.

This is a far more mundane picture than fears of cyber theft conjure. Hacking and IT incidents accounted for just 5 percent of breaches, or just 2 percent of people affected by breach during the period.

The incidents covered the period from September 2009 to November 2010. The breaches were reported between February 2010 and January 2011.

Hardware, Data Unsecured



More than half of all large-scale data breaches reported to the federal government in the past year resulted from the theft of computers, portable media, and records. Hacking was involved in just 5 percent of incidents.

Final Rule Expected Next Month

Organizations have been reporting breaches under a federal rule on breach notification that took effect February 2010. The rule resulted from one of several privacy-related provisions in the American Recovery and Reinvestment Act of 2009.

Under the rule, organizations must report all breaches of unsecured protected health information to Health and Human Services at least annually. Breaches involving 500 or more people must be reported within 60 days. The department posts these reports publicly at www.hhs.gov/ocr/privacy/hipaa/administrative.

Organizations must also notify the individuals whose information is breached.

The industry is currently working under an interim final rule. Next month the government expects to release a final rule. The most watched-for provision will be the so-called harm threshold, which under the interim rule allows the organization to determine whether a breach represents significant risk of harm to the individuals involved. If the organization determines the risk of harm is slight, it may forego notification.

The threshold is intended to reduce administrative burden in instances where little risk of harm exists. However, those opposed to the provision argue it reduces transparency and that such a decision should not be in the hands of the organization.

More at http://journal.ahima.org.

Watch for news of the final breach notification rule on the *Journal of AHIMA* Web site.

Article citation:
AHIMA. "Swiped, Not Hacked: After a Year of Reporting, Theft Remains Main Cause of Breach" *Journal of AHIMA* 82, no.2 (February 2011): 66.
