Low-Tech Security Risks Still Leading Cause of Breaches

Save to myBoK

By Harry Rhodes

Low-level technology risks continue to be the leading cause of reportable data breaches, according to a review of the Office for Civil Rights' security breach statistics for breaches affecting more than 500 patients.

An analysis of OCR breach statistics conducted by the Health Information Privacy/Security Alert revealed an increase in the number of reported breaches caused by theft that affect more than 500 people. The breaches increased from 179 to 193 between May 17th and June 17, 2011, while the number of security incidents that resulted in the loss of protected health information (PHI) accounted for 65 reportable breaches.

Lost and stolen laptops continue to be the most common type of security incident, accounting for 75 reportable incidents.Not only have theft and loss of PHI continued to dominate the category, there has been an increase in both of these security incident categories.

The February 2011 Journal article "Swiped, Not Hacked: After a Year of Reporting, Theft Remains Main Cause of Breach" reported that lost and stolen laptop, desktop, and network server equipment continues to be the leading cause of large-scale breaches reported to the Department of Health and Human Services, contrary to widespread fear that attacks by malicious hackers represent the greatest threat to electronic health information.

Security Audit Guidance

In February 2011 AHIMA updated its "Security Audits of Electronic Health Record" practice brief to provide members with resources and guidance on the components of a successful security audit strategy. Organizations can mitigate some security risks by having an active audit process.

In AHIMA's "Security Risk Analysis and Management: An Overview" practice brief, industry expert Tom Walsh examines the regulatory requirements that are the basis for an effective security risk analysis. He also offers suggestions for how to conduct a risk analysis.

In addition, a few simple safeguards can prevent the theft or loss of your laptop, mobile device, and the valuable data stored on it:

1. Never leave your laptop unattended. Keep it guarded when attending a business meeting or using your laptop in a public place. When at the airport (especially at the curb) don't ever set your laptop carrying case down. Teams of thieves commonly work the arrival and departure curbs.
2. Attach identification to your laptop. Attach your business card to the laptop with a piece of clear postal packing tape. Many individuals lose their laptops going through airport security or even at crowded meetings. Laptops all look the same.
3. Invest in a cable lock. Use it to secure your laptop to a table, desk, or chair. Consider using the cable lock in your office, as 40 percent of laptops are stolen from the office.
4. Invest in office security cameras. Brazen thefts have been known to walk right past the reception desk with a stolen laptop—you may have even held the door for one.
5. Limit the amount and type of sensitive information on your laptop.
6. Use only password-protected USB storage devices.
7. Disable USB ports. To prevent unauthorized file transfer onto USB storage devices, IT security managers have either removed or in some cases glued USB ports shut.
8. Disable wireless infrared file transfer.

9. Password protect the basic input-output system (BIOS). All modern BIOS configurations support password protection and are designed to be the first code run by a PC when powered on. The initial function of the BIOS is to identify, test, and initialize system devices such as the video display card, hard disk, floppy disk, and other hardware. Although this protection can be circumvented, password-protecting the BIOS can prevent someone from changing the BIOS and from booting the system without using the password. In addition, configure the BIOS to boot first from the hard drive.
10. Use a Windows OS password. Many laptop manufacturers ship systems with the standard Windows welcome screen and no password, leaving it up to you to protect your system. Your first step upon getting a new laptop should be to open the control panel and click “User Accounts.” Select your user account and click “Create a Password” to password-protect the system. While you’re in the “User Accounts” window, it’s also a good idea to disable the guest account.
11. Don’t automate VPN connection scripts. Most companies have set up VPNs so that traveling employees can access corporate resources. Companies should also require a manual log on for all VPN connections. Automated log-ons make it too easy for laptop thieves to gain access to corporate data.
12. Consider tracking software. Some fairly new security applications enable your laptop to “phone home” if it’s stolen. Some programs can report a laptop’s physical location when it connects to the Internet; others can automatically delete sensitive data.
13. Encrypt the file system. Encrypting the file system can ensure that the sensitive information on your laptop stays private even if the device is lost or stolen. Windows XP lets you encrypt the sensitive data on your system, thus keeping data safe even if a thief installs a new OS to gain access to the computer.
14. Use a personal firewall. Losing your laptop isn’t the only way to lose the information on it. If you’re connected to a public network—or even an unfamiliar private network—your laptop and the data on it are potentially open to viruses as well as unauthorized access. Using Windows Firewall or another personal firewall, is the first line of security for protecting the data on your laptop from unauthorized network access.

Additional Resources

AHIMA. “HIPAA Privacy and Security Training (Updated).” November 2010.

AHIMA. “HIPAA Security Overview (Updated).” November 2010.

AHIMA. “Information Security—An Overview (Updated).” December 2010.

Privacy Rights Clearing House. “Chronology of Data Breaches: January 10, 2005–Present.”

Original source:
Rhodes, Harry B.. "Low-Tech Security Risks Still Leading Cause of Breaches" (Journal of AHIMA website), July 19, 2011.

Driving the Power of Knowledge