Your Organization's Data Theft Hot Spots Revealed, Part II

Last year, Kroll Advisory Solutions offered a list of "data-rich locations" found in offices around the world.

The list consisted of primary areas within the organization—such as employee desks and workspaces, unlocked filing cabinets, and mobile devices—that are easy targets for data thieves. This year, we thought we'd update the list with the latest vulnerabilities, as well as some new twists on the tried and true.

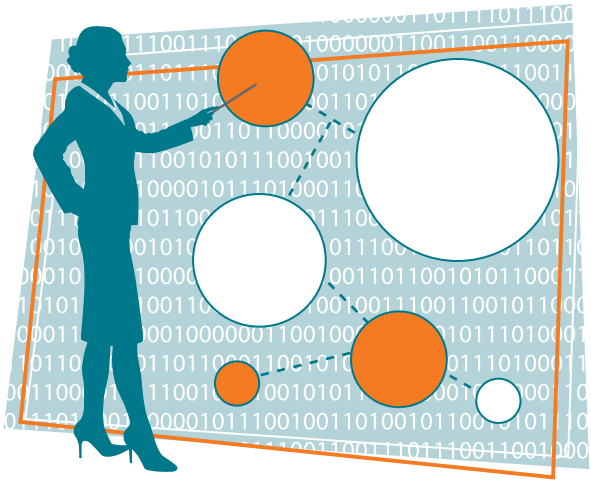
When comparing corporate data security threats between 2011 and 2012, we reconfirmed the old adage: the more things change, the more they stay the same. Although the data theft landscape has changed considerably in the last year, many of the preferred modes of attack remain actively present. The only difference? Data thieves are packaging them in a new wrapper.

The following are some of this year's common areas of compromise and Kroll's advice for what you can do to detect and defeat the threats against them:

UPDATED: Laptop computers and mobile devices

Why they're hot: Laptops have always been a major source of data breaches, which is why they made last year's list, but the proliferation of mobile devices has caused this issue to explode for many organizations. The healthcare industry is a perfect example of this—according to the 2012 HIMSS Analytics: Security of Patient Data, 31 percent of respondents indicated that portable device use was among the factors most likely to contribute to a breach, up from 20 percent in 2010 and four percent in 2008. Also, the popularity of Bring Your Own Device (BYOD) has opened the doors to new technologies in the workplace with new security holes that may not be as tightly monitored by your IT team.

How to minimize your risk: If you permit employees to BYOD at work, certain minimum levels of security must be agreed to; otherwise, the employee should not be allowed to access the network. Best practices include



device access control through passwords; use of specific, company-approved security software; and company access to remotely destroy data if the device is ever lost or stolen. In most instances, the convenience and popularity of BYOD with employees far outweighs any inconvenience brought on by added restrictions.

NEW: Voicemail systems

Why they're hot: Everyone has voicemail, and most systems use little more than a 4-digit password for access. There have been highly-publicized voicemail system breaches, where unauthorized individuals were able to crack the password and gain access to the user's voicemail, including private company information. In some systems, the unauthorized user can actually listen to messages and reset the system to appear as though the messages had never been accessed.

How to minimize your risk: Voicemail, much like email or faxes, is a recorded communication and thus should fall within your organization's data security and privacy guidelines for employees (as it does for those of healthcare entities bound by HIPAA privacy rules). Guidance should include details on what type of information is/is not acceptable to include in a voicemail message. Never allow

users to continue using default passwords like "1234." If possible, use a password that is longer than 4 digits. Here, access logs are also important: if it's an option, make sure you are logging the date and time that messages are accessed to better help users identify questionable periods of use that may signify unauthorized access.

NEW: Conference Calls

Why they're hot: Phone and video meeting capabilities are vital communication tools, but we find that many employees have the habit of using the same conference call bridge number and access code over and over again, particularly if the meeting occurs regularly. This can leave your virtual sessions vulnerable to access by unwanted guest, including employees, ex-employees and possibly hackers who gain access to your call-in information.

How to minimize your risk: If an employee leaves the company (particularly those joining a competitor), be sure to change the access codes for any meetings he or she regularly attended. Make certain that employee is removed from the distribution list for meeting invites as well. In all cases, opt to receive a report at the end of the conference call that gives details on the number of dial-ins to help you to identify any "stowaways" on your call.

UPDATED: Mailrooms

Why they're hot: We previously deemed mailrooms a hot spot due to the amount of sensitive information entering the company via mail, but while we're at it, let's flag the material leaving your premises, as well. We've seen cases where insiders were able to exfiltrate media storage devices through the mailroom, by simply placing them in a standard USPS box and putting them with the outgoing mail.

How to minimize your risk: Know where your data resides and place appropriate-to-their-job limits on employees' access to it. Restrict the ability to download the information to personal devices by blocking access to USB ports or other means of retrieval. In the case mentioned, the employee had access to "old" backup tapes that were considered obsolete because they had been replaced by newer ones—yet the unencrypted tapes were still available and still contained valid data.

NEW: Your employees

Why they're hot: Although implied in the previous hot spot entries, employees should certainly be considered as targets in their own right, particularly given their role in securing and interacting with sensitive data. A few high-profile breaches in the last year were the result of social engineering tactics, like spear phishing, that took aim at employees with the intent of duping them into doing something they should not.

How to minimize your risk: Employee privacy and security awareness training (including third-party vendors and contractors) builds security equity and enhances your employees' ability to recognize the signs of an attack or threat. Beyond this, organizations must step up their intrusion detection and prevention methods, strengthening their monitoring and logging activities and blocking attacks with web filtering.

Today's thief is after the same thing as yesterday's thief—your valuable data. While they're willing to work hard to get at it, mostly they look for the path of least resistance—attacking the data sources that aren't on your radar, haven't been updated, and aren't well protected. The best defense is vigilance. Something as simple as a delay in installing critical software updates can open the door to a successful attack. Mistakes will happen, but keeping an eye on data theft hot spots will go a long way towards preventing a breach.

For more insight from our team of professionals, be sure to visit Kroll's blog "A Dialogue on Data Security."

www.krollfraudsolutionsblog.com

Kroll Advisory Solutions℠

For more information, call or visit us online.

866.419.2052

www.krolladvisory.com