Your Organization’s Data Theft Hot Spots Revealed

Data thieves know the most data-rich locations within your organization... do you?

Too often, businesses large and small think of data security as strictly an IT department concern. They lull themselves into a false sense of complacency, believing that a significant investment in virus software and other cyber security measures has effectively eliminated their risk of a data breach.

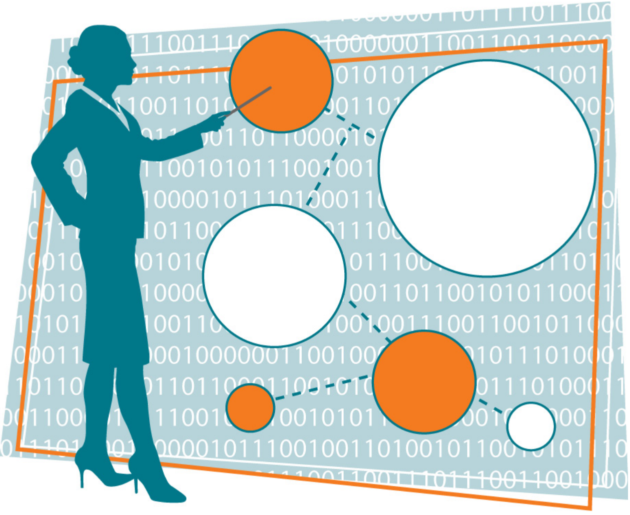
The truth is that the loss, theft, or misuse of sensitive personal information (SPI) can happen anywhere within your organization. There are a number of “data theft hot spots” that aren’t secured behind a firewall. They may not even be secured behind a locked door! In fact, negligence remains the most common threat, and an increasingly expensive one: According to the Ponemon Institute’s *2010 Annual Study: U.S. Cost of a Data Breach*, 41 percent of breaches were attributable to negligence. The cost of those breaches averaged $196 per record, up 27 percent from 2009. Don’t let your organization be just another statistic.

Below, Brian Lapidus, chief operating officer of the Information Security, Forensics and Data Breach division of Kroll, identifies six primary data theft hot spots and what your organization should be doing to protect them. See if any of these are on your organization’s radar:

Laptop computers

Why they’re hot: Laptops can house a lot of SPI (worse—unencrypted SPI) pertaining to your organization, personnel, and clients. They also provide a gateway to your organization’s server, where a far greater amount of data is stored.

How to minimize your risk: First, make sure all data is encrypted and all laptops are password-protected. Then, implement a policy for laptops that explains what type of information can be stored on them and reminds employees to purge unnecessary data from laptops before taking them from the building.



Employee desks and workspaces

Why they’re hot: Employees may leave unsecured SPI piled up on the desk or in unlocked drawers, offering easy access for a thief. Additionally, recent surveys have shown that, regardless of motive, departing employees tend to take information with them.

How to minimize your risk: Implement a “clean desk” policy across your organization and perform periodic audits to ensure that all workspaces are secure and in good working condition. For example, broken locks and lost keys should be replaced promptly, and employees should be encouraged to report any such incidents as quickly as possible. These sound security practices can easily fall by the wayside over time, so it is important to offer a “refresher” to employees from time to time. Be sure to reiterate that documents created or kept by employees are still company property and, as such, cannot be taken if an employee leaves for whatever reason.

Unlocked filing cabinets

Why they’re hot: Filing cabinets are often the storage of choice for hard copy records that contain employee, customer, and vendor SPI. Failing to lock the cabinets—even if they are located in a secured area—increases the chances that this sensitive information could get into the wrong hands.

How to minimize your risk: The short and obvious answer is “lock them up!” but take your solution a step further by regularly evaluating the files they contain and disposing of any unnecessary information. If you don’t have it, you can’t lose it. Plus, locking down SPI also sends the message to employees that this is valuable data and should be treated as such.

Emails and faxes

Why they’re hot: Outbound SPI is always vulnerable because the company no longer has control over it. Plus, data in transit is easily intercepted, and even inbound information (e.g., faxes left on the machine for anyone to pick up, incoming emails left in view at an unlocked computer station) can pose an issue.

How to minimize your risk: Make sure all employees understand what kind of SPI can and cannot be sent out via email or fax. If certain SPI must be sent via email, consider having employees send it in a password-protected document, and make sure all electronic correspondence contains the company’s confidentiality clause. Remind your employees that emails are retrievable records subject to discovery in a court case.

Mailrooms

Why they’re hot: Plenty of SPI comes and goes through the mailroom, making it a target for internal and even external threat, depending upon the level of security.

How to minimize your risk: In today’s environment of heightened physical security, the mailroom has become more important as companies work to keep employees safe in the event dangerous substances are sent through the mail. Generally speaking, your safety plan will contain useful elements for securing SPI, too. Restrict mailroom access only to employees that need it and use keycards or sign-in sheets; and make sure mail deliveries are made to a secure, restricted area.

The trash

Why it’s hot: Outbound data does not need any particular destination to be vulnerable to threat—even SPI that is being disposed of can be stolen.

How to minimize your risk: Make sure shredders or a locked disposal box are readily available for employees so that they have no excuse not to safely dispose of sensitive information. To avoid any confusion, ensure that all staff members are properly trained as to what constitutes sensitive information and how they can and should dispose of it.

If companies fail to communicate that they are serious about data security, employees won’t take it seriously, either. Encourage your staff to discuss ways that the company can make the job of securing information as easy as possible. While no office can totally prevent the loss, theft, or misuse of data, determining data theft hot spots will go a long way toward increased awareness and optimized data handling practices.

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

www.krollfraudsolutionsblog.com

Kroll®

For more information, call or visit us online.

866.419.2052

www.krollfraudsolutions.com

Certain Altegrity companies provide investigative services. State licensing information can be found at www.altegrity.com/compliance. These materials have been prepared for general information purposes only and do not constitute legal or other professional advice. Always consult with your own professional and legal advisors concerning your individual situation and any specific questions you may have. © 2011 Kroll, Inc. All rights reserved. Item #THT-022-2011-9-20