Harvard Business Review

HBR Blog Network

The Most Overlooked Part of Your Data Security

by Kyle Marks | 10:30 AM June 14, 2013

Organizations constantly replace outdated computers, servers, laptops, copiers, and countless other types of electronic devices to keep up with technology and enhance worker productivity. This rush to upgrade, however, creates a challenge: large numbers of excess electronics must be managed and disposed of properly.

During a recent IT asset disposal project for a large New York bank, a chain-of-custody audit revealed three computers were untracked. An IT director was suspected of taking them.

When first questioned about the missing systems the IT director — let's call her "Robin Hood" — denied any knowledge. Next she blamed the disposal vendor for taking an inaccurate inventory. Then she accused a truck driver of stealing the systems en route to the recycling facility.

Finally, when confronted with evidence, Robin admitted that her daughter's elementary school was in desperate need of computers — but insisted that, as a 12-year veteran of the firm, she would never intentionally harm her employer. She said she had ensured the hard drives were erased, and pointed out that the bank had historically donated used computers to nonprofit organizations. But what she viewed as a trivial act was in fact a serious data security threat that created massive liability for her company.

A Rising Threat

Securing sensitive data is a daunting task for any business. Today more than 550 US laws now affect IT asset disposition. Data security laws mandate that organizations implement "adequate safeguards" to ensure privacy protection of individuals. And the penalties for data breaches are tough. Under a proposed data protection law, European firms could face fines of up to 2% of their annual turnover for a breach. The HITECH Act enacted in 2009 extended provisions surrounding information handling and increased penalties for HIPAA violations. Today, American companies are subject to unprecedented sanctions following HIPAA security violations.

Governments are not the only ones eager to punish violators. The effect of a punitive privacy class action lawsuit can be far worse than a government fine. Following the loss of a backup data tape in 2011, US healthcare benefits provider TRICARE was hit with eight separate privacy lawsuits, including one seeking an astounding $4.9 billion in damages. The company was accused of "intentional, willful, and reckless disregard of plaintiffs' privacy," and for failing to respond to "recurring, systemic, and fundamental deficiencies in its information security." Similarly, Sutter Health was hit with a billion dollar suit, and Emory Healthcare faced a $200 million suit.

Historically, privacy class actions have faltered due to the plaintiffs' inability to prove recoverable damages; however, this provides little consolation for a company being sued. The cost of defending privacy suits can cost millions. The average litigation defense now exceeds $500,000 and the average settlement is over $2 million. Moreover, corporate risk managers should take note of recent decisions in the US Eleventh Circuit Court of Appeals that bring punitive class actions closer to becoming big payoffs for plaintiffs (and, of course, their attorneys).

Savvy plaintiff attorneys are also shifting legal tactics. In addition to defending themselves against claims for damages, violators must now defend against claims that they unjustly profited by skimping on security safeguards that could have prevented a breach in the first place.

Soft Underbelly of Data Security

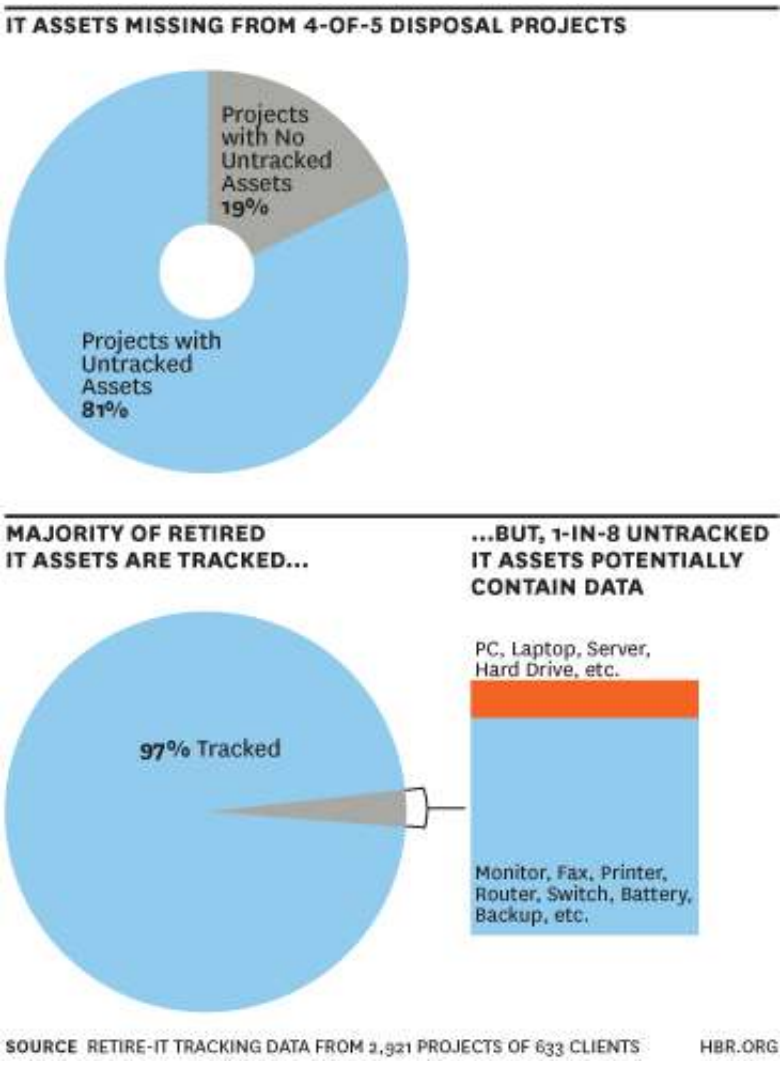
Without question, most large organizations take data security seriously. Corporations will spend an estimated $68 billion worldwide this year on IT security measures including firewalls, network monitoring, encryption, and end-point protection. When an organization spends millions guarding against hackers, it is tempting to feel confident.

But the most overlooked aspect of corporate data security may be simple IT asset disposition — in part, ironically, because so many businesses now rely on expert assistance. The fact that certified electronics recyclers are transporting retired IT assets to vendor facilities to be processed and sanitized can create a false sense of security that blinds executives to the biggest threats. First, there is still the possibility that assets can be lost or stolen in-transit. (Increasingly, companies are learning to destroy data in-house, prior to disposal; that way, any loss or theft, while unfortunate, won't result in the financial disaster that would come from an actual data breach.) Second, there is the threat we saw with our Robin Hood IT director: Trusted insiders can take retired assets any time before the handoff to the outsourcer, and before data is destroyed.

For the past eight years, Retire-IT has been tracking how effective security-conscious organizations are when it comes to accounting for retired assets.

At a high-level, organizations might seem to do an adequate job with chain-of-custody. On average 97.2% assets were tracked.

Detailed tracking data, however, reveals a troubling fact: four out of five corporate IT asset disposal projects had at least one missing asset. More disturbing is the fact that 15% of these "untracked" assets are devices potentially bearing data such as laptops, computers, and servers.



(http://blogs.hbr.org/cs/assets_c/2013/06/assetdisposal-4224.html)

Chain-of-custody is not a catchphrase: It is the foundation for indemnification and transfer of liability. It only takes a single missing item to cause a breach. Only a careful, objective examination of tracking data can confirm chain-of-custody — or reveal potential liability.

How can a business keep a Robin Hood from taking retired computers, and potentially making a plaintiff attorney's dream come true? Acknowledging the risks and inherent conflicts-of-interest surrounding retired assets will result in more effective ITAD policies and adequate safeguards. Applying established incident-response procedures to the process of ITAD can help raise awareness of unappreciated vulnerabilities. Educating senior management about the risks will hopefully secure IT asset managers the resources needed to prevent an ITAD-related breach.

A critical aspect of every major data security law is that organizations must minimize segregation-of-duties conflicts that create opportunities for theft and fraud. Treating IT asset disposal as a "reverse procurement" process will deter insider theft.

There will always be people and places, like Ms. Hood's local elementary school, that could use free computers. Make sure the way they obtain them doesn't cost your company billions.
