PHOTODISC

Crime in the workplace

Protecting your business from identity theft

By Scott Steinberg

A HARVARD UNIVERSITY honors graduate and head of a thriving start-up, Costco member John Sileo was a smashing success 10 years ago. But then his entire life changed with a knock. At the door: an investigator for the Denver district attorney's office, alleging that Sileo had stolen $300,000 from his clients.

Like hundreds of other people and organizations, from businesses to government agencies, each year, Sileo and his company had been the victim of identity theft. But in this case, it was for the second time—courtesy of his former business partner. More frightening still, as the *Privacy Means Profit* (Wiley, August 2010) author and professional speaker warns, if it can happen to him, it can happen to anyone—including you and your business.

"Even the most seemingly innocent data, such as names, addresses and employment histories, are at risk," Sileo cautions. "While the media likes to talk about high-tech methods of data theft, the reality is that most crimes occur the same way they did 10 years ago: through human error. Every office is filled with potential hazards, from unshredded reports to computers left logged into private networks and sensitive documents that somehow end up in the trash."

Having been victimized through his own negligence (forgetting to destroy personal mortgage documents) and naiveté (allowing an untrustworthy associate to manage his firm's accounting), Sileo can't stress the importance of caution enough. Because even when justice is served, as in the case of his onetime partner, who went to jail for just 18 days and has since returned to private commerce, it's often scant compensation for the loss of one's reputation or customers' trust.

Hazards in the workplace

Sensitive data can provide a windfall to crooks, with targets including bank account numbers, credit-card info, customer data and employee records. Intellectual capital, ranging from a family restaurant's secret recipe to a firm's client list, is also valuable to thieves.

Points of vulnerability are many—from unshredded financial statements to out-of-date antivirus programs to stolen laptops that don't possess software encryption. Nor is your own desk safe anymore, as documents left on it overnight may fall victim to an unscrupulous member of the cleaning staff.

Armed with just names, addresses and phone numbers, thieves can often con or compute their way into enough information to register credit cards, run up bills and otherwise wreak havoc in your company's name.

Such incidents can be costly. The average cost to an organization of recovering from a data breach hovers at $6.75 million, according to Javelin Strategy & Research. That doesn't count loss of productivity, customer goodwill or brand equity. Just ask Sileo, who spent more than 500 hours recovering his good name, suffered untold humiliation, had to rebuild his entire credit history and lost his family's 40-year-old business.

Smart steps for prevention

"An ounce of prevention far outweighs a pound of cure," says Sileo. He recommends several strategies to guard against data loss.

- Conduct employee background screening and reference checks, including researching the credibility of supporting references.
- All computer equipment that your business uses, including hard drives, laptops, USB keys and smartphones, should be encrypted and equipped with a password.
- Shred sensitive documents—don't just throw them in the garbage.
- Create a corporate culture that supports preventative measures. Offer employees basic training that clearly illustrates the risks of not taking regular precautionary steps, and make it simple and convenient to take part in the process.

"Part of the problem's due to ignorance, some of it stupidity, and you also have to throw in some apathy and lack of awareness," Sileo sighs. "People assume that they can protect their systems."

But with inside theft, dodgy software protection (beware of unsecured WiFi hot spots, which hackers can monitor) and clever cons (a healthy fear of unsolicited e-mails and calls helps), it's wise to take precautions. As the commercial sector moves more toward wireless solutions ("Never use the same password for multiple purposes") and cloud computing ("Beware trading redundancy and scalability for control of your data"), you can never be too paranoid.

"Just think like a spy," says Sileo. "It never hurts to maintain a healthy sense of suspicion, or plan ahead."

The Costco Connection

Costco sells a variety of shredders and security software in the warehouses and online at Costco.com. Also, Costco has teamed up with IDENTITY GUARD® to offer two identity-theft products—Credit Protection and Total Protection. Go to Costco.com and click on "Services" for more information.

Scott Steinberg is the head of high-tech consulting firm TechSavvy (www.toptechexpert.com).