PHOENIX Business Journal

SUBSCRIBER CONTENT: Nov 26, 2006, 10:00pm MST

Tool Kit

Even without big budget, employee theft can be stopped

Kathleen Davidson
Contributing Writer

Ever wonder where your profits are going?

The U.S. Chamber of Commerce estimates that theft by employees costs American companies $20 billion to $40 billion a year.

The 2005 FBI Computer Crime Survey further supports these staggering figures, reporting that 44 percent of respondents experienced serious intrusions from within their own organizations.

The data support the experience of Arizona Assistant Attorney General Gail Thackeray, who said, "If a company is a victim of a financial crime, odds are great that the perpetrator is an employee or a consultant."

Equally disturbing, Thackeray said, is that "embezzlement likely is the work of a trusted, long-term employee." Recognizing that internal fraud is common, Thackeray expressed shock at the number of companies that fail to have non-disclosure and information security agreements.

"While small businesses may not have large staffs, they still have tremendous legal exposure by operating without these agreements and a solid internal security system," said Thackeray.

Johnson Bank Corporate Security Officer Susan Wisneski agreed, noting, "Businesses of all sizes need to provide a written code of conduct that spells out expectations and clearly states that every allegation of wrongdoing will be investigated and could lead to termination and criminal prosecution."

This is particularly important for firms dealing with medical records and real estate transactions, Thackeray said. "They are vulnerable and must use offsite backup."

In addition to addressing the well-covered crisis of identity theft (Arizona still ranks at the top nationally), Thackeray pointed to the overall need for the right firewalls and routers to cover opportunities presented by high-speed Internet access. This particularly applies to wireless users.

Thackeray suggested small firms use and back up two hard drives and take one offsite because, "Small companies can be ruined if trade secrets and customer data are stolen."

Vincent Liu, a partner in the Stach & Liu professional security services firm in Phoenix, preaches controls.

"Digital information is great, but it allows faster transfer of pirated information. You have to control who has access," said Liu. "Just like a locked file cabinet, sensitive information should be 'locked' with 'key' access. Provide the least access needed for each person to perform their job.

"Protecting your data comes down to managing your people, processes and technology, but the real key is the people. They are the X-factor," said Liu. "In addition to checking references and conducting background checks, make every effort to talk to former superiors, peers and subordinates."

Bob Parsons, senior vice president with security responsibility at Johnson Bank/Arizona, empathizes with small business owners who have limited time and money to spend on security. "Dual controls are crucial," he said. "Make sure you have one person signing checks and a different person reconciling the books."

"Small business owners may think it is too costly to implement controls," said Wisneski, Johnson Bank's corporate security guru. "In reality I've seen it nearly cost owners their business when they fail to do so."

Wisneski suggested the following simple but critical steps:

- Determine risks
- Develop controls to limit risks
- Write appropriate policies/ procedures
- Monitor effectiveness and fine-tune accordingly.

Local certified public accountant Randy Elder recently took his security efforts up a level by implementing an e-mail encryption system that requires a "security key."

An ardent advocate of hardware firewalls, Elder said, "You'd be surprised at the number of clients I've had who only have a software firewall and no anti-virus or anti-spyware program installed." For those who do, he suggested using a service that updates such software on a regular basis.

Elder also uses a private portal to transmit his backup data to secure sites which he learned are located in underground bomb shelters designed to withstand an atomic blast. He strongly encourages small business owners to backup data to a tape, external hard drive, or online service because, "It may save their business one day."

Get connected

Stach & Liu: www.stachliu.com

Randy Elder, CPA: www.eldercpa.com

Johnson Bank/Arizona: www.johnsonbank.com

FBI 2005 Computer Crime Survey: www.fbi.gov/page2/jan06
/computer_crime_survey011806.htm