



Small business: protecting company data

April 4, 2011 by JAMIE HERZLICH / jherzlich@aol.com

A breach of privacy for any company can prove devastating, particularly if it involves the leak of sensitive information regarding customers and employees.

It's a critical issue for many small businesses, according to a 2010 [Symantec Information Protection Survey](#) that found almost three-quarters of small and mid-sized businesses are concerned about the loss of crucial business information and 42 percent have actually lost confidential or proprietary information.

Given the threat, it's never too late to update your privacy policies and practices to protect your company and key stakeholders, say experts.

"Failing to protect the data you handle inside your business every day will affect your business," says John Sileo, author of "Privacy Means Profit" (Wiley; \$24.95) and president of ThinkLikeaSpy.com, a [Denver](#)-based data theft and fraud prevention site. "It's not if, it's when it will affect it."

About eight years ago, Sileo said, his 40-year-old family-owned [software](#) firm was put out of business because of identity theft and a data breach after his login credentials were stolen by an associate to access clients' [bank information](#) and transfer \$300,000 from their accounts.

Simple steps like not keeping his password visible on his monitor and having auto lock on his screen saver could have helped prevent his loss, said Sileo, who started his present business to help others avoid the same fate. "Most identity theft and data breach can be traced back to a bad human choice," he says.

To protect your own company, consider these safeguards:

Conduct a security audit: Know what information you're trying to protect and have an outside accountant or consultant assess the quality of your security, including password, virus and spyware protection, says Sileo. Be sure to include penetration testing of your Internet presence, adds Robert Bagnall, chief executive of Maverick Cyber-Defense in Washington, D.C.

Train staff: Make employees understand how identity theft impacts them personally on an individual level before you move onto the corporate side, says Sileo. Show them strategies for protecting their own data, such as shredding, as well as corporate data. "You have to show them the value of their data as an individual before you can expect them to care about protecting the company data," he notes.

Establish policy: Companies should have a written policy in place on privacy and nondisclosure of information, says Felix Nater, president of Nater Associates in Freeport, which specializes in workplace security. The policy should include what information can't be disclosed, as well as

ramifications if there's a breach, he notes.

Safeguard information: Passwords shouldn't be left in visible places for everyone to see, says Nater. All sensitive records should be encrypted or password-protected, and sensitive documents should be under lock and key, he notes. It also pays to change your passwords periodically, says Kevin Beasley, chief information officer at VAI, a business management software provider in Ronkonkoma.

VAI does that and enforces password policies, such as not allowing employees to have an easily guessable trivial password. VAI trains employees on how to pick a new password, which includes having special character/number requirements. "We take security very seriously because it's important to our customers," says Beasley.

Limit access: Just because you have 20 employees doesn't mean they all need access to the same information, says Bagnall. Control the flow of information, as VAI does. "People have access to what they need to have access to," he says.

Conduct annual reviews: Keep current on industry requirements and federal regulations, says Nater. Run an annual review of security procedures and policies, suggests Bagnall. "Understand what you need to be compliant with," he notes.

Fast fact Small and midsized businesses are spending, on average, \$51,000 annually on information protection, including computer security, backup recovery, etc.

Source: [Symantec](#) 2010 Information Protection Survey

[< back to article](#)