

## **SECURITY ISSUES FOR EVERY COMPANY**

---

From January 22, 2007  
Business New Haven Journal



**Gail Benson**  
**Director, IT Risk Management**  
**Fiondella, Milone & LaSaracina LLP**

### **By Karen Singer**

It's no secret that small and mid-sized companies are just as vulnerable to losing vital business data as the big guys. Despite that, they're less likely to do risk assessments and take preventive measures to protect themselves.

"It's difficult to get people to spend money on something that hasn't occurred or if they don't think they have a problem," says Frank E. Rudewicz, managing director for UHY Advisors in Hartford. "But they end up spending much more money reacting than [they would] if they had done a routine security audit."

"Smaller organizations often think, 'No one is going to attack us,'" says Jeffrey Ziplow, a partner at Blum Shapiro Consulting in West Hartford. "But the reality is the hacker doesn't know whether it's a small or large company. A lot of times they just scout around." Moreover, smaller companies may not realize that the most damage is often done by employees.

The American Society for Industrial Security's (ASIS) 2006 Trends in Proprietary Loss Survey of Fortune 100 companies "showed the No. 1 threat was internal," Rudewicz says, and that risks have increased through "exploitation of trusted relationships, including vendor, customers, joint ventures and subcontractor/outsourced providers."

According to a 2005 survey by the Ponemon Institute, which tracks information and privacy management practices in business and government, 69 percent of data breaches were made by insiders - and 39 percent of data breaches had to do with confidential business information.

The institute's 2006 National Survey on Managing the Insider Threats concluded the three top threats to data integrity were "missed or failed security patches on critical applications, accidental or malicious insider use of sensitive or confidential data and virus, malware and spyware infections."

What often happens when a company has lax security is "hackers find their site, modify their system and use it for storage of stolen property," says Kenneth Lacasse, information technology director for Shelton-based Security Services of Connecticut (SSC). "Or they use it for spamming and could be sending hundreds of thousands of messages per day and it looks like it's your system."

"I had one server recently that had probably eight different copies of French-dubbed DVDs of popular movies like Mission Impossible 3, [and the hacker was] using a good amount of their space," Lacasse adds.

Unmonitored remote access can likewise increase vulnerabilities.

"We had a situation with a client where remote access was authorized and it was turned on, but no one was aware it allowed other unauthorized persons to access e-mail," Rudewicz says.

*To guard against such risks, smaller companies*

*“really need to spend some time in overall planning,” advises Gail Benson, director of IT risk management at Fiondella, Milone & LaSaracina in Glastonbury. “The two biggest areas where I find companies have exposures are [unauthorized] people can get in [to their networks] and they may not have [the protective measures] the business really needs to have in place.”*

During planning, companies should identify the proprietary information they most want to protect and “adopt policies and agreements to protect it,” explains Shawn Kee, a partner at Jackson Lewis in Stamford. Such policies could include non-disclosure and non-competition agreements with employees.

Employers must decide “who should have access to what and review employees’ access periodically to make sure no unauthorized changes have occurred,” Benson says.

Employees should be given “only as much access as they need to get their job done; they don’t need to be poking around,” adds Lacasse. “But at a lot of small companies, they give full access to everybody.”

*Benson says a “well-defined access plan” also should be checked by people in charge of information generated by various parts of business to make sure data hasn’t been changed by somebody hacking in or an unauthorized insider.*

*“The same thing applies with firewalls,” she adds. “You could have a very good firewall, but if you don’t have the other controls around it, there could be ten people with access who could change it and you might not know who did it.”*

*Safeguarding company secrets also hinges on proper password protection.*

*Benson suggests passwords be at least eight characters long and not be easy to guess, or find. “I’ve seen them posted on computer screens with a sticky note, or under the keyboard,” she says.*

*Passwords also can be problematic because people often use the same name and password to access different accounts.*

*“We had a case where someone got into an executive’s personal bank account and was making transfers,” says Lacasse.*

Spyware or malware (malicious code variations) sometimes turn up when Lacasse is doing internal company audits.

*“You could have something hosted on your internal network supplying information to someone outside your network,” he says. “Or you may get some kind of virus or spam mail that actually installs something on your computer and allows someone to get more information about your system.”*

Software devices also can be embedded in e-greeting cards, which will send an e-mail to the person who sent it.

Lacasse recommends other security precautions, including making sure employees log off when they’re done for the day and changing the default setting on a wireless router as soon as you plug it in.

Smaller companies also should set up policies and procedures on employee monitoring and privacy restrictions, especially in Connecticut, which in 1998 became the first state to pass a statute protecting the electronic monitoring of employees.

*“This mainly requires that employers post a notice of what type of electronic monitoring they may do, and that they put out other forms of notice there may be electronic monitoring,” Kee explains. “It’s important that employees sign an agreement which makes clear that the company’s technology is an employer’s property and not the employees.”*

*Benson says such a policy should spell out an employee’s obligations regarding the use of technological assets, including e-mail, voice mail, Internet use or access.*

*“I generally like to see it signed, which puts a company in the better legal position,” she adds.*

*Benson also recommends using software to block access to Web sites companies don’t want employees to visit and prohibiting the use of thumb drives, those small portable USB devices that can store several gigabytes of information (and facilitate theft of data).*

*“At a minimum, you should be getting updates to your PCs; those are free,” she says. “You should stay current with the software on your desktops and laptops. If you use vendor software to do financials, you need to be able to evaluate updates and figure out when to install them. You also should stay current with virus protection, installing strong, anti-virus software that’s automatically updated.”*

*Some companies already conduct routine financial audits to make sure they’re in compliance with federal laws such as the Gramm-Leach-Bliley Act, which pertains to privacy and protection of financial data, Sarbanes-Oxley, which provides safeguards to assure businesses cannot deliberately or accidentally commit fraud and the Health Insurance Portability & Accountability Act (HIPPA), which requires health-care organizations to maintain patient information in separate files.*

James K. Robertson, a partner at the law firm of Carmody & Torrance in Waterbury, points out businesses of all types and sizes should be paying attention to new federal rules regarding preservation of electronic information. The rules, which became effective on December 1, concern the discovery process in a lawsuit, which is the way parties exchange information.

“Companies cannot ignore this,” Robertson says. “What these rules will do is require all businesses to preserve electronically stored data as soon as it is likely there is a dispute, and more significantly, will require them to produce that data to their opponent.

Moreover, he adds, “We’re not talking just about PCs. We’re talking about anything that

electronically stores information, including employees’ home computers, PDAs [personal digital assistants], voice-mail servers, digital voice recorders, camera phones, instant messaging and thumb drives.”

Smaller companies interested in improving their computer security might want to check out the ASIS “Information Asset Protection” guideline, which provides advice for employers and other entities on “collection, storage, dissemination and destruction” of companies’ information assets, including proprietary information, trademarks and privacy information. (Go to [www.asisonline.org](http://www.asisonline.org) and click on “Guidelines” on the left side of the screen.)

UHY Advisors’ Rudewicz, who helped draft the ASIS guideline, stresses information protection should be part of an overall company security plan that includes physical security protection as well as contingencies for business continuity.

“Security is not a one-shot deal; it’s an evolving process,” Rudewicz says. “Just as you do a financial audit on an annual basis, you should be doing periodic audits of your network security so you have a pulse check of your risks and what your vulnerabilities might be.”

UHY Business Development Manager Jake Lyons expresses similar sentiments.

“The key is to make sure your business goals match your technology infrastructure,” he says, “and most important, to test against these things. New threats come out every day.”