

Locking out cyber criminals

Companies are protecting themselves and their customers as the threat of cyber attacks increases.

By Suzanne Stevens

Dave Johnson was trying to make a prudent business decision when he chose Linux as the mail server for his new Portland-based Web development company, Netropole, six years ago. Even though Netropole was a Microsoft solutions provider, Linux and its free mail service were an attractive option over a high-cost Microsoft system. What Johnson didn't realize was that, like most systems, Linux had a few holes. And that, left unpatched, those holes made the company's server vulnerable to a hacker attack.

"We get a phone call from a credit card clearinghouse company asking what their credit card information is doing on our server," says Johnson. That call was followed by one from the FBI. "We came to understand that somebody had hijacked our server and used it for storage of illicit material."

The attack didn't affect Netropole's bottom line, but it could have. The company, which has since added computer security to its list of services, could have been sued.

Eighty-five percent of Internet security managers surveyed by the San Francisco-based Computer Security Institute reported computer security breaches at their companies last year. And the situation is expected to worsen in the aftermath of Sept. 11. President Bush has appointed a cyber-terrorism security chief, and the FBI's National Infrastructure Protection Center warned of increased threats to the nation's computer networks.

While threats to computer security may

seem a world away to a small manufacturer in, say, Southern Oregon — which might think it's flying under the radar of cyber attackers — that's not the case. Smaller companies, which often have fewer defenses than larger ones, may be even *more* appealing as easy targets for hackers looking to hone their skills.

"The potential for loss is even greater," says Johnson. "If a small- to mid-sized business gets their accounting system wiped out or it gets hijacked, it's the end of the line in some cases."

And if your company's server or website is used for illegal purposes, as happened with Netropole, your company could be held liable for any damages even if you were unaware of the security breach.

"If it does occur, and you've taken no measures to prevent it, your liability exposure is rather large," says David Marosi, owner of the Vancouver-based investigative firm The Marosi Group.

PROTECTING DIGITAL ASSETS — proprietary data, strategic plans, client and employee profiles — doesn't have to be difficult or expensive. And while some suggestions might seem obvious, the rise of computer security breaches and the spread of Internet viruses indicates we could all use a refresher on even the most basic security measures.

One of the simplest is to have employees shut down computers when not in use. Think of it as locking your doors. If a thief shakes the doorknob and finds it locked, he's more likely to move on.

If a hacker does break in, a creative

password can keep him at bay. Never use the default setting that comes from the manufacturer. A hacker that guesses your password — and there are dictionary programs that try out thousands of words looking for a match — has just picked your lock.

You should also make daily backups of important information and store them offsite.

Remind your employees (again) not to open e-mail attachments from strangers, and regularly update virus protection soft-

double whammy of federal warnings about cyber terrorism and Nimda have spurred companies to take action.

"When I talk to people about putting in a \$3,000 to \$5,000 firewall, there used to be an argument. Now awareness is up, and it's not a big argument."

A firewall, which monitors and separates your internal system from the outside, is a must if your company has a direct connection to the Internet. An industry-certified firewall can be purchased for as little as \$400, according to Johnson.

Having two servers offers another layer of protection by allowing the company to store valuable information on a server with no link to the outside.

"We don't have any Internet access from our second server," says Alix Nathan of the Portland-based Mark Spencer Hotel, which began taking online reservations through its website in June. Customer credit card numbers that come in through the website and the hotel's other proprietary data are stored on the second server, protecting it from an outside attack.

Companies that have telecommuters face additional challenges. While information is making its way to the employee's home computer, it is unprotected. It's a good idea to evaluate what information telecommuters are authorized to send back and forth and what they have stored on notebook computers.

While firewalls, virus protection and dual servers work to protect networks from prying outsiders, the FBI estimates that as many as 80% of cyber threats come from a company's own employees. Meaning, it's critical to know *who* you're hiring. (See INVESTIGATIVE HIRING, p. 48.)

RESOURCES

Information Systems Security Association: www.issa.org

National Infrastructure Protection Center: www.nipe.gov

Security Focus: www.securityfocus.com

Carnegie Mellon Emergency Response Team: www.cert.org

Systems Administration, Networking and Security Institute: www.sans.org

ware. Norton, McAfee, Sophos and Trend Micro are all industry-certified.

These simple steps can save millions in downtime. Estimated damages from last year's Love Bug e-mail virus range from \$6.7 billion to \$15 billion, and the nation is still calculating losses due to Nimda, a sophisticated virus that posed a lethal and unprecedented threat.

"It had knowledge of e-mail, it had knowledge of network topology, it had knowledge of operating systems," says Netropole's Johnson, who adds that the

OUR LIPS ARE SEALED

Think your company has no trade secrets worth stealing? Think again, says John Stevason, head of the Intellectual Property and Internet Practice group at the Portland law firm Lane Powell Spears Lubersky.

"[Trade secrets] are not limited to what most people think of as technical things. It's what makes that business unique, what gives them their competitive advantage," he says.

That could be information about employees, clients or products. It's information worth protect-

ing, and here are some ways to do that:

- Have new hires sign confidentiality and nondisclosure agreements that state employees will be exposed to trade secrets and that it is their obligation to maintain secrecy.
- Have new hires or promoted employees with access to proprietary data sign noncompetition agreements, preventing them from taking trade secrets to competitors when they leave the company.
- Conduct exit interviews with outgoing employees reminding them of their legal obligation to

PROTECTING YOUR DIGITAL ASSETS

- Create an incident response plan before something happens.
- Regularly remind employees about security policies.
- Use strong passwords.
- Make regular backups of critical data, and store it offsite.
- Use virus protection software, and update it regularly.
- Install a firewall if your company has a direct connection to the Internet.
- Take computers offline when not in use.
- Don't open e-mail attachments from strangers.
- Store sensitive company information on a server with no outside link.

"Trust, but verify," suggests Marosi, whose company is hosting a workshop in Portland this month on counter-terrorist strategies for businesses. (Visit www.marosi.com for details.) And don't just rely on references provided by the job candidate. Look for holes in a person's résumé, says Marosi, or hire a private investigator or human resources agency to review the résumé of anyone who will have access to trade secrets or proprietary data. **OBM**

If you have comments about this article, e-mail us at feedback@oregonbusiness.com.



A victim of cyber attack himself, Dave Johnson of Netropol now helps other businesses protect digital assets.