Los Angeles Times | ARTICLE COLLECTIONS

← Back to Original Article

Small firms learn size doesn't matter to hackers

Companies of all sizes find they need protection from cyber attacks. For some, the realization comes only after being victimized.

May 23, 2011 | By Cyndia Zwahlen

It took all of three minutes for the hacker to break into the small accounting firm's computer system.

The virtual open window into the system turned out to be a computer equipped with outdated software. It provided access to the office network and the hacker was able to get files that included private financial information.

"That was a shock," said Lynne Leavitt, a partner at the four-person Los Angeles firm, Brakensiek Leavitt Pleger. "I thought we had good security. I thought we were safe."

Luckily, it was just a test. The hacker had been employed by a security company to test the accountants' digital defenses. As a result, the firm put in new software and adopted new security procedures.

Cyber security is not just for big businesses. "That's one of the myths we come across — 'I am too small,'" said Stan Stahl, head of a Los Angeles cyber-security company Citadel Information Group Inc. and president of the Los Angeles chapter of the Information Systems Security Assn., a trade group.

At a cyber-security conference last week sponsored by the Federal Communications Commission, the government agency cited a 2010 survey by Symantec Corp. of small and medium-size companies. Symantec, which sells anti-virus software, said that about 73% of the businesses in the study reported they had been targets of cyber attacks in the last year.

Michelle Marsico, who owns Village View Escrow Inc. in Redondo Beach, was hit hard.

Last year, $465,000 was stolen by hackers from one of her business bank accounts, Marsico said. The thieves may have gotten some of the data they needed to access the account by invading the computer system at her small company.

After gaining access, the hackers directed the money to be wired overseas, she said. About a fifth of the money was recovered.

Marsico has spoken out about what happened to her so that others can be forewarned. "I am determined to make a difference so this doesn't happen to anybody else," she said.

Taking precautions against cyber thieves not only is an act of self-protection but also might be a requirement for winning new clients.

An increasing number of corporations are requiring that companies they hire as contractors, no matter how small, have digital defenses in place. This is especially true in the healthcare and financial services industries, where consumer privacy laws are being strengthened.

"It's a competitive advantage" to have privacy protections in place, said Bessie Ramirez, a principal at Santiago Solutions Group, a 10-person consulting firm in Studio City that counts Fortune 500 companies among its clients.

Even if a hacker attack does not result in funds being stolen, a security breach can be costly to a business if customers' financial information is exposed. Laws in many states, including California, require that every person whose information might have been compromised must be notified. In some cases, these customers must be offered some form of digital protection for a certain amount of time in case a hacker eventually tries to use the private data.

"The average cost per breach for notification under today's law is roughly $250 for each customer that has to be alerted," said Dana Coates, president of Pasadena-based United Western Insurance Brokers. If just 2,000 customers have their confidential information exposed, that adds up to $500,000.

Cyber insurance is available, but installing at least some protections can prevent a lot of headaches. Winn Schwartau, president of Security Awareness Co. in Old Hickory, Tenn., recommends businesses make sure an electronic firewall is in place and regularly updated.

"The first thing you want to do is be invisible to the Internet," he said. "The way you do that is to make sure you have a firewall that gives you stealth capability. That way the bad guys can't even see you."

No data security system is fail proof — companies as huge as Sony Corp. have been hit with cyber break-ins recently. But you don't want to be an easy target.

"You will never prevent someone who is set on getting you," Leavitt said. "But you will prevent people from randomly getting you because you are the weakest link."

smallbiz@latimes.com