Newsday
newsday.com
THE LONG ISLAND NEWSPAPER
May 12, 2014

TAKING STEPS TO cybersecurity

Survey: 30% of attacks targeted small businesses

SMALL BUSINESS
Jamie Herzlich
jherzlich@aol.com

Data breaches at large companies like Target and Michaels grab headlines, but that doesn't mean small businesses aren't at risk.

A recent Symantec survey found that 30 percent of targeted cyber-attacks in 2013 were aimed at small businesses, and targeted attack campaigns grew 91 percent, year over year, across all industry sizes.

"A lot of small businesses get lulled into a false sense of security," says Brian Burch, vice president of global consumer and small-business marketing at Mountain View, California-based Symantec, which specializes in information protection.

Small businesses are often seen as easy targets and can also be viewed as a gateway to gain access to a larger company's data, says Burch. Many small businesses are suppliers to larger companies, and hacking into them to gain access to a corporate giant can be easier than hacking into the big company itself, he explains.

A Pennsylvania heating and air-conditioning contractor may have provided the opening that hackers exploited in last year's massive breach of Target's computer network.

Data breaches expensive

"It's way past the time that you could put your head in the sand," says Steve Rubin, a partner and co-chair of the new cybersecurity practice at Moritt Hock & Hamroff LLP in Garden City. "If you're not protecting your business, you could go out of business."

He says the new practice, which launched in January, took shape as he monitored the trends and "saw a lot more data breaches — and how problematic and expensive they can be for businesses."

NEWSDAY / AUDREY C. TIERNAN

Steve Rubin, a partner and co-chair of the new cybersecurity practice at Moritt Hock & Hamroff LLP in Garden City, warns: "If you're not protecting your business, you could go out of business."

FAST FACT

94%

Percent of small firms that say they're very or somewhat concerned about cybersecurity, while 1 in 4 have little to no understanding of cybersecurity issues.

Source: National Small Business Association 2013 Small Business Tech Survey

The most common types of attacks against small businesses in 2013 were spear-phishing, in which a legitimate-looking email contains a link or attachment that launches a virus, malware or spyware, and ransomware, a type of malware that restricts access to your computer and demands a ransom or fine be paid to restore access, the Symantec survey found.

The first instinct when a breach occurs is to call in a tech company, says Rubin. But he advises clients to call legal counsel first, because anything the tech firm uncovers is "potentially discoverable in a litigation. " If you call an attorney first, the attorney could hire the tech consultant on your behalf, and the information he or she receives could potentially be protected under attorney-client privilege, he notes.

If customer data is exposed, a company should be able to show it took reasonable measures to protect that data, Rubin says. "You need to be able to say 'We did the best we could in light of the sensitivity of our data and the potential for a breach.' "

Also consider getting cybersecurity insurance, which could help cover expenses such as legal fees, he notes.

Ways to secure networks

But how do you protect your firm from suffering a breach in the first place?

Do a cybersecurity audit, says Rubin. Identify where your sensitive data is and who has access to it, both internally and externally, to assess vulnerabilities.

Keep operating systems current with the latest security products and updates including anti-virus and anti-malware programs, says John Gonzales, director of engineering and support services at A+ Technology and Security Solutions in Bay Shore. The company's security systems can monitor for physical breaches, but also can detect cyberbreaches in client companies' computer networks, says A+ president David Antar.

It's important that companies secure their networks internally as well as externally, to avoid employee-triggered breaches, he says.

Limit access to data to employees who need it. Keep passwords secure and not easy to guess, notes Gonzales. And don't skimp on firewall protection, he says.

Keep sensitive data encrypted, adds Burch. Inexpensive encryption programs are available that make data difficult to read if hacked.

And educate employees to watch for fraudulent emails and not open suspicious attachments or links, says Gonzales.