ADVISEN CYBER RISK NETWORK
Insurance Intelligence for the Cyber Community

FEBRUARY 14, 2014

As easier marks, small companies besieged by cybercriminals

By Chad Hemenway

Criminals of any kind typically seek vulnerabilities in security—a tendency holding true among criminals within the cyber realm.

The bad news for small-to-medium businesses (SMBs) is that cybercriminals are looking at them and seeing weaknesses to exploit.

According to Symantec's 2013 Internet Security Threat Report, 31 percent of all targeted attacks were aimed at businesses with less than 250 employees. That is a threefold increase from 2011. In 2012, 50 percent of all targeted attacks were aimed at businesses with fewer than 2,500 employees, Symantec added.

Larger organizations have become more difficult to crack after investments in security and breach recognition. This is making SMBs the path of least resistance.

"Criminals have moved on to smaller or mid-sized companies because they are the most vulnerable," Tim Francis, enterprise cyber lead at Travelers, told Advisen.

The reasons are not difficult to surmise. Smaller businesses often lack the technology know-how, a dedicated information technology department, data security measures or devoted legal advice. Not to mention, software is usually not up to date.

A survey of SMBs from McAfee and Office Depot last year found 80 percent of SMBs do not use data protection and less than half use email security. About 90 percent do not use security to protect employee's mobile devices.

"It's hard to say how often small businesses are breached due to not reporting or underreporting," Toby Levy, head of technology at Hanover Insurance. "They might not understand they are being hacked, or not even be aware."

Typically, SMB owners have an attitude that cyber data breaches happen to larger peers—that hackers wouldn't waste their time attempting to breach a small company without the breadth of personal or intellectual data or information as is held at larger companies.

That necessarily isn't true and statistics have shown it. Nevertheless selling cyber insurance to SMBs has always been a challenging proposition. Raising awareness and convincing business owners the coverage is worthy of the expenditure hasn't been easy. Initial cyber insurance product offerings were not geared toward SMBs, said Levy.

"Products weren't exactly small-business friendly and it's always challenging finding the right balance," Levy said.

Another survey from The Harford concluded nearly 40 percent of small businesses owners do not think there would be an impact on their business even if they experienced a data breach.

continued ▸

However, the recent data breaches of larger corporations have revealed another cyber liability for SMBs. Some say a breach of Fazio Mechanical Services, a refrigeration vendor in Pennsylvania, led to Target Corp.'s, point-of-sale malware attack late last year that has led to as many as 110 consumers having credit and debit card or personal information stolen.

Fazio confirmed it was the victim of a cyber attack but an investigation continues into whether and how one breach led to another. Experts have differing opinions. Regardless, can vendors be held responsible, or liable, if their data breach is responsible for the breach of its larger business partner?

"Sure," answered Francis. "I think there could be a healthy attempt to stick liability to a vendor [in this type of situation]."

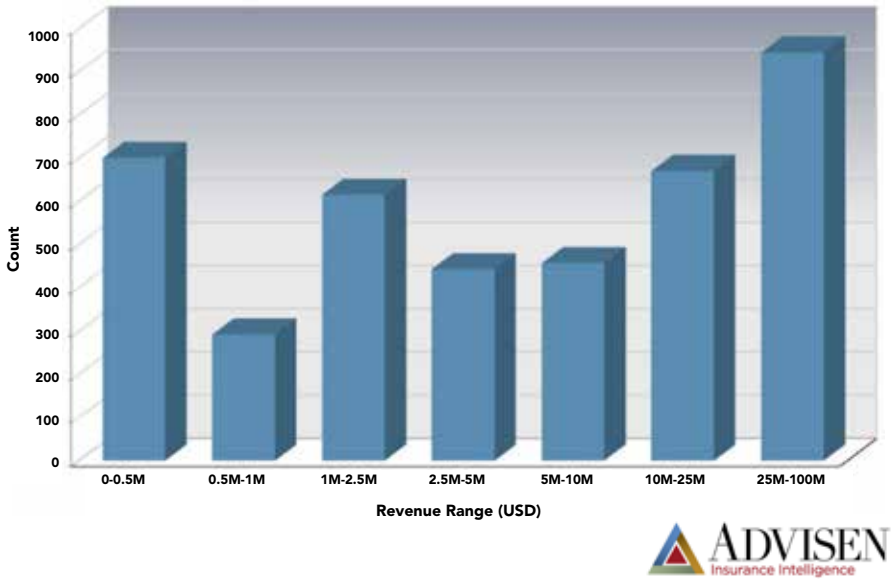
Symantec reports, "Attackers deterred by a large company's defenses often choose to breach the lesser defenses of a small business that has a business relationship with the attacker's ultimate target, using the smaller company to leap frog into the larger one."

Francis said large companies may require its vendors to have insurance in place. Contractual language like this has existed, but could increase in light of recent third-party hackings leading to breaches up the chain.

Larger partners could file suit against smaller vendors but Levy pointed out, "They don't have deep pockets." Nevertheless, he added, "These situations carry exposures and costs."

"It's an eye-opener for everybody," Levy continued. "We're all surprised."

ADVISEN LOSS INSIGHT SNAPSHOT: SMALL BUSINESS CASE COUNT



So instead of hitting a wall — a perceived affirmation of the it-can-only-happen-to-large-companies myth — insurance providers and sellers can used the latest news to highlight yet another cyber risk to small businesses.

"It isn't easy to identify small," Francis stated. ""It really has nothing to do with your exposure, as we have seen. It all depends on the data you have and whether it is worth something to someone else."

Advisen's Loss Insight holds more than 4,000 cyber-related cases from businesses with revenues of up to $100 million. The case counts appear to support Francis' comment, as business with revenues of only up to $500,000 have one of the highest case counts of this grouping.

Francis said cyber insurance was a hot topic before the recent flurry of high-profile breaches. "This has just added to it," he said.

Levy said he recently spoke to local agents and asked about cyber-insurance buzz.

"The dialogue seems to have increased with Main Street businesses," Levy reported. "This is an opportunity for agents to truly showcase their expertise."

Smaller companies usually do not have risk managers on staff. In recognition of this, insurers like Travelers and Hanover have enlisted partners.

Travelers with NetDiligence last year launched a suite of online resources to help business owners navigate the growing threat of cyber risks while also protecting their assets and their customers' information.

Hanover has a partnership with IDentity Theft 911.