Cybercriminal strikes can be small, but mighty

Stephanie Schiraldi, The (Nashville) Tennessean *July 22, 2014*

Cybercrime is a growing threat for businesses as attackers are getting more creative and skilled in their methods of stealing information.

Cyberattacks on large companies such as Target, Neiman Marcus and P.F. Chang's made headlines across the country and affected millions of consumers. Verizon's 2014 Data Breach Investigations Report even tagged 2013 as the "Year of the Retailer Breach."

Small to midsize businesses are just as big a target for cybercriminals as larger companies are. *(Photo: Getty Images / iStockphoto)*

However, what most don't realize is that small to midsize businesses are just as big a target as larger companies.

John Mensel, director of security services at Concept Technology in Nashville, said the biggest question he is asked by clients from smaller businesses is, "Am I really a target?"

"My answer is emphatically 'yes,' " he said. "You're not only a target, you are being actively attacked."

Many small-business owners believe they are under the radar, but Mensel said this mindset can be "very dangerous."

Parker Rains, vice president of the Southern-based insurance firm Fisher Brown Bottrell, agrees.

"Just because your business is a small fish, doesn't mean you're too little for an attacker to care about," Rains said.

continued next page

A report by cybersecurity firm Symantec showed that businesses with fewer than 250 employees represented 31 percent of all attacks in 2012.

Most of these smaller businesses are only focusing on good firewalls and anti-virus software. But according to Mensel, “Here in 2014, that’s not enough.”

Typical anti-virus software cannot detect intrusions, and attackers are targeting smaller businesses because they know such firms do not have as much protection.

“Attackers are staying several steps ahead of the tools we are using to detect them,” said Mensel. “As a result, I’m seeing businesses where they’ll have compromises on their systems for months that have gone undetected.”

Attackers work fast

According to Verizon’s DBIR, it takes attackers only a few days to breach a business, but fewer than 25 percent of breaches are discovered in that short amount of time.

“That’s the No. 1 problem in network security today,” Mensel said. “Attackers are compromising networks very, very fast, and as IT people, we are not doing a good job at detecting them.”

However, Verizon’s DBIR also said internal discovery of attacks outnumbers external discovery for the first time in the report’s history. Mensel said this shows “we are coming to terms with the problem, but we still have a long way to go.”

There are many steps businesses can take to protect themselves against attacks, Rains said, adding that cybercrime is not covered by general business liability insurance.

He said what all businesses actually need is cyber liability insurance.

“There’s not one type of business that’s more likely to be attacked,” Rains said. “Everyone is susceptible to it.”

Businesses are at risk for five types of cybercrime: unauthorized access, network damage, human error, theft of digital assets and cyber extortion.

Rains said cybercrime insurance is very affordable and can save a business “thousands of dollars in future fees and expenses.”

“It’s not going to shut (businesses) down because they have to pay a new premium,” he said. “Never would those penalties and costs (associated with a breach) exceed what a policy premium would be.”

continued next page

Breaches expensive

The Ponemon Institute's 2013 Data Breach Study showed the average cost of a data breach in the U.S. is $188 per record lost or stolen.

Rains said most insurance policies cover notification in the event of a loss of protected information; crisis management to pay for the firms that maintain and/or restore customer confidence; regulatory proceedings such as fines and penalties; and credit-monitoring expenses for victims of the breach.

Rains added that cyber liability insurance can even cover HIPPA violations if medical information is breached.

For smaller businesses that may not have a large IT budget, Mensel said the question typically becomes, "How do we pick our battles?"

However, when a company decides to buy cyber liability insurance, Rains said it can tailor the policy to its specific business needs.

How to protect your business

1. Have an inventory and know where it is and how to protect it. "Above all else, if you don't know what you have, you can't defend it," says Mensel. "Know what assets you have that a thief would want."

2. Let the offense inform the defense. "Only protect yourself against the real threats," Mensel says. "It's so easy to spend time and money protecting against things that aren't there."

3. Prevention is important, but detection is a must. "We want to prevent people from successfully breaching our networks, but detection is essential and we are totally failing at that," says Mensel.