Cybersecurity: An ever-changing battleground

MAY 14, 2015

What began as a game for petty hackers has become big business for organized crime and a platform for nation-states with a grudge. Cybercriminals are exploiting the anonymity of the Internet to commit a range of crimes, and businesses need to adopt new tactics, and soon, because problems are multiplying.

The 2015 Global State of Information Security Survey by PwC found that of 9,700 business leaders said the number of detected cyber incidents reached 42.8 million in 2014, a 48 percent leap over 2013. Resulting financial losses were 34 percent higher than in 2013.

And stakes are rising: The number of respondents reporting losses of $20 million or more almost doubled over 2013.

The Center for Strategic and International Studies estimates the annual cost of cybercrime and economic espionage at over $445 billion, or nearly 1 percent of global income. While it is difficult to accurately measure economic losses attributable to cybercrime and trade secret theft, another PwC study estimates the economic impact measures between 1 and 3 percent of GDP.

However, some businesses are discouraged by high-profile breaches that have occurred even with security measures in place.

“I hear it from executives quite a bit — they feel like they’re fighting a losing battle. No matter how much they invest, breaches continue to happen,” says Joe Nocera, a PwC principal who heads the cybersecurity and privacy practice for the firm’s financial services sector.

In the meantime, spending on security has actually decreased, the PwC study found. Investment in information security declined about 4 percent in 2014. Despite recent high-profile breaches, fewer than half of those surveyed said their board actively participates in security strategy.

Danger signals

Two trends have combined to make cybercrime more ominous, Nocera says. First, Internet touch points have increased through the use of social media, phone banking and the Internet of Things — Internet-connected devices and home appliances that communicate with one other.

Second, hackers have become more sophisticated. Big breaches are no longer likely to be the work of geeks looking for an intellectual challenge. Instead, perpetrators fall into four categories: organized crime rings motivated by financial gain, nation-state players motivated by national policies or the advancement of state-owned businesses, politically motivated “hacktivists,” and vengeance-motivated disgruntled or corrupt insiders.

Sophisticated criminals

Crime rings package stolen credit card and Social Security numbers into bundles of hundreds or thousands and sell them on websites for a few days before the theft becomes public and card owners start canceling.

And these rings are difficult to shut down.

“Criminals have become very good at knowing where safe havens are,” Nocera says. They use servers in countries hostile to the U.S. “In some cases, we can find out the street address of individuals responsible, but it can be a place not friendly to the U.S. – which limits what law enforcement can do to take action,” he says.

So what are businesses to do?

“Nothing you do can make you 100 percent safe, but there are several important steps businesses should take,” Nocera says.

1. Communicate and cooperate within your industry. One of the most important strategies is sharing information about cybersecurity with others. The financial services and aerospace industries, which are targeted the most, were the first to pool information and strategize about solutions, and others have followed in their footsteps.

Some companies report they are hiring people with a government intelligence background to piece together the types of threats that are likely in their environment.

2. Analyze network traffic data. Businesses have another cybercrime-fighting tool at their fingertips: big data. Firms collect mountains of information on network traffic and characteristics of website visitors. The trick is making sense of it all.

Increasingly, businesses are hiring data analysts to look for the dangerous needle in a haystack. It could be a user who normally logs in between 9 and 5, but starts using the site at 3 a.m., or a user who suddenly increases the volume of transactions.

Data can also be used for behavioral analysis to prevent insider fraud. Certain triggers — a big decline in credit score, a bad review, a destabilizing life event, or frequent travel to countries hostile to the U.S. — may make it more likely for an employee or contractor to turn rogue.

Workflow can also be measured for danger signs. Someone who handles 2,000 customer records a day while peers manage 100 is raising a red flag.

3. Better training and policies. As if businesses didn’t have enough to worry about, a new potential frontier for cybercrime is emerging from the Internet of Things. It’s a particular worry for the healthcare industry, which is increasingly connecting patient mobile devices to those of doctors, clinics and pharmacies.

“What concerns me is that a threat actor could have the ability to harm a large number of people,” Nocera says of the new devices.

Healthcare organizations, which are governed by strict federal data privacy rules, need to ensure all participants in information-sharing receive adequate and updated training. Executives should take an active interest in cybersecurity, monitoring trends and adjusting policies along the way.

No silver bullet

Regardless of how hard businesses fight cybercrime, it will never disappear.

In that respect, it’s no different from other kinds of crime. Perhaps retailers could prevent 100 percent of shoplifting if they used metal detectors and kept merchandise under lock and key. And banks could cut credit losses to zero if they stopped writing loans. But who wants to live in that kind of world?

Dealing with cybersecurity effectively means defining your risk tolerance. You can’t prevent every security breach, but developing good tactics for detection and rapid response will go a long way toward minimizing damages.

—Teresa Meek, Tribune Brand Publishing