CREDIT UNION MAGAZINE

Prepare now, because cyberattacks will happen

http://news.cuna.org/articles/112366-prepare-now-because-cyberattacks-will-happen

Jennifer Woldt | May 26, 2017

Take steps to prevent attacks, but also to respond and recover.

"People think of this as things from spy movies," retired FBI special agent John Iannarelli says of corporate espionage, "but it's a real issue."

The question is no longer if a cyberattack will happen at your credit union. Instead, it's when an attack will happen and if the credit union is prepared to respond, according to a panel of experts at CU Direct's Drive '17 Conference.

"The great big elephant in the room if you're a credit union is cybersecurity and what really happens when you have a breach," says Jim McCabe, senior vice president, identity theft services with VERO. "The reality is, it can still happen even if you do everything you can to prevent it from happening."

Some of the top cybercrime trends include:

- **Identity theft**. More than $50 billion is lost annually due to identity theft. And while 50% of reported identity thefts are related to a financial event—such as stolen credit card or bank information—the remaining attacks are related to nonfinancial events, such as taxpayer identification fraud and theft, medical identification, or a credential identification—driver's license, passport, or student ID—theft, says Mark Pribish, vice president and ID theft practice leader with Merchants Information Solutions.
- **Phishing and ransomware**. It only takes one employee to click a suspect link in an email to launch a phishing attack at your workplace.
- **Business email compromise**. In these attacks, an attacker targets employees by posing as a boss or supervisor and wants money transferred. Eight hundred businesses were victims to these types of attacks during the last two years, with losses over $1.2 billion.
- **Corporate espionage**, or stealing a company's ideas. "People think of this as things from spy movies," says John Iannarelli, a retired FBI special agent, "but it's a real issue."

Only 25% of all cyberattacks are a result of information technology and hacking though. Seventy-five percent of all data breaches are the result of inside threats. And according to a study by Symantec, 43% of all breaches happen at businesses with less than 250 employees.

When a data breach occurs, it costs an average of $221 per lost customer records.

Mark Pribish

“Your members are fearing what they’re hearing when it comes to data breaches,” Pribish says. “These things are becoming nightmares for members.”

While it’s a good move to offer monitoring services for your members, that’s only a “smoke alarm” when it comes to addressing and fixing cybercrime, Pribish says.

Instead, consider finding a “fire extinguisher approach,” or ways to provide a fully managed recovery service for those who have become victims. These services extend to the victim’s family, covers all forms of identity theft, have no limits to returning the victim to their preattack status, and provides services upon suspicion alone.

Also look for programs that offer credit monitoring or expense reimbursement services.

“Look for the fire extinguisher approach, but also those ancillary items as well,” McCabe says.

“Look for the fire extinguisher approach, but also those ancillary items as well,” McCabe says.

KEYWORDS breach / cybersecurity / data / Drive 17