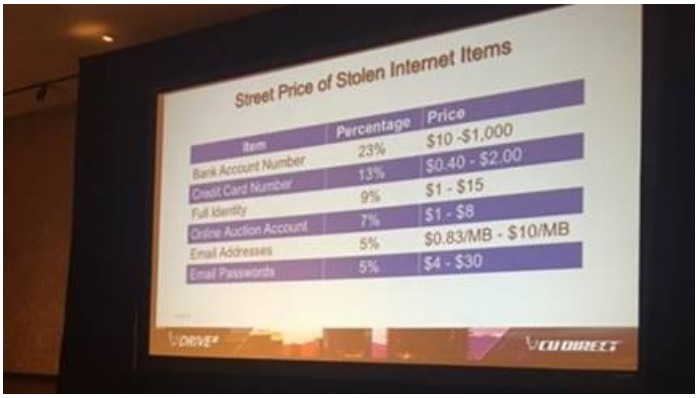
Credit Union Times

Breach Management Must Focus on Response, Recovery: CU Direct's Drive

http://www.cutimes.com/2017/05/25/breach-management-must-focus-on-response-recovery?slreturn=1495777208

By Natasha Chilingerian
May 25, 2017



Speakers explained what hackers earn on the black market for personal information they steal online.

LAS VEGAS – Due to advancing technologies and a growing amount of internationally-connected data floating around in the world, credit unions and other organizations can be considered powerless in their quest to stop all breaches in their tracks. Instead, they should invest their time and resources into response and recovery plans to put into action when the inevitable attack occurs.

That was the key point three cybersecurity experts brought home during the breakout session "**Data Breach Risk Management: Real Risks, Real Data, Real Answers**" at CU Direct's Drive conference Thursday.

Retired FBI special agent **John Iannarelli**, Merchants Information Solutions VP and Identity Theft Practice Leader **Mark Pribish** and Vero SVP, Identity Theft Services **Jim McCabe** shared staggering statistics on the rise of cybercrime, including a 270% increase in business email compromises in 2016, a 16% increase in identity fraud since 2015 and a cost to organizations of $221 per record stolen.

"Think of 9/11 – when the buildings came down, we had billions of dollars in damage. We're having a 9/11 of cybercrime every year in the U.S.," Iannarelli said.

Iannarelli identified seven of the largest breach trends as identity theft, phishing, ransomware, business email compromises, breaches stemming from BYOD policies and corporate espionage. He said to develop a successful recovery plan, credit unions should first identify what information they consider sensitive and critical to protect (public information on the credit union's website, for example, may not be worth protecting). Next, a plan for recovery – headed up by the credit union's key decision-makers, not the IT team – should be put in place. Iannarelli noted credit unions shouldn't assume their IT professionals are always doing the right thing as they may not be on top of the hacking trends. Finally, credit unions should establish a relationship with the FBI so they'll know who to contact in the event of a breach.

Response plans should cover the 48 hours following a breach, McCabe said, and include messaging to victims that will deter them from wanting to sue you, as well as a notification procedure that is fully compliant with the credit union's state and federal breach notification guidance.

Pribish pointed out that 75% of all hacks, whether intentional or accidental, originate from insiders – current and former employees, customers, associates, vendors and independent contractors – and agreed that a swift breach response plan is mandatory.

"The answer is response and recovery," Pribish said. "If you're talking this morning about an event that happened last night, you're already too late."

He added that 50% of all reported identity theft is related to a financial event, and credit unions should keep their eye on the top two forms of identity theft: Tax fraud and medical identity theft.

McCabe explained that credit union members are very concerned about identity theft and how it might affect them if they become victims, including the reputational repercussions and the work it might entail to get their lives back in order.

He recommended that credit unions implement comprehensive identity protection services to help their members protect themselves. In addition to setting up a credit monitoring service, which McCabe described as a "smoke alarm" in that it only alerts members when their information has been stolen, credit unions should invest in a fully-managed recovery and restoration service from a third party (or, a "fire extinguisher").

In searching for the best program from a third party, McCabe said credit unions should ensure it covers all forms of identity fraud, as well as family fraud and elder fraud – the latter of which swipes $40 billion from senior citizens annually. As additional services, credit unions should consider offering expense reimbursement insurance, and credit score and reporting services. And the services should also be offered to credit union employees, not just members, he added.