What Can RIAs Learn From the Biggest Cyberhacks of 2015?

February 29, 2016

Last year's spectacular cybersecurity attacks are more than just headline-grabbers, they are a reality check for advisors who believe they could never be targeted for a hack. It is worth a look at a few of these breaches so that registered investment advisors (RIAs) can understand the keys to preventing similar incidences from crippling their firms and devastating their clients.

J.P. Morgan And Other U.S. Financial Institutions

Dubbed the largest theft of customer data from a U.S. financial institution in history by prosecutors, J.P. Morgan was attacked repeatedly from the same source from 2012 to 2015, resulting in the theft of data and personal information of more than 80 million customer accounts. The thieves were also responsible for cyberattacks into six other major banks, Fidelity Investments, online brokerage firms ETrade and Scottrade, software companies and financial news sites such as Dow Jones, the parent company of The Wall Street Journal. The thieves made and laundered millions of dollars resulting from these attacks through a vast online network that included fake antivirus schemes, pump-and-dump stock schemes, Internet casinos and a Bitcoin exchange.

U.S. Office Of Personnel Management

The attack on the U.S. Office of Personnel Management (OPM) is one of the biggest breaches ever of U.S. government systems, with the addresses, social security numbers, fingerprints, health and financial details of nearly 22 million people stolen during the summer of 2015. The head of the agency resigned in July 2015, and its chief information officer resigned in February 2016. Though it has never been publicly confirmed, Chinese hackers are believed to be responsible.

FBI Portal Breach

In November, the Law Enforcement Enterprise Portal shared by FBI and the police was hacked by the same cyberthieves believed to be responsible for breaking into CIA Director John Brennan's personal email account earlier in the year. The hackers accessed information on arrestees as well as data from private email accounts of FBI Deputy Director Mark Giuliano and his wife. The exact numbers were not disclosed, but the attack has been characterized as one of the biggest law enforcement breaches of 2015.

Though these high profile attacks happened at organizations that could deliver a high return on investment for the cyberthieves, it is a mistake for advisors to assume that they are off

the hacker radar screen because they are too small to be worth the risk. One RIA managing $500 million in assets may not be incredibly lucrative to an enterprising hacker seeking a profit on the dark web, but 100 RIAs with $500 million in assets each certainly are. A single firm managing the wealth for a select number of very high-profile individuals and families is similarly desirable. As the J.P. Morgan and FBI portal attacks show, hacks do not necessarily happen as one-time, siloed events, and may take months or years to fully reveal the extent of their damage within an organization or industry.

These hacks underscore that when it comes to cybersecurity, what is being done today is not enough. With today's open systems and proliferation of Web-based applications, RIAs need policies and tools that can address breaches. Additionally, regulatory compliance can add another layer of complexity for RIAs who want to lock down their systems. So if organizations with deep pockets cannot protect themselves, what is a growing RIA to do? For starters:

Encrypt and secure all email. As both the OPM and FBI portal breaches demonstrate, email is the preferred hacker entry point. The RIA's first defense against cyberattacks is to encrypt and secure all inbound and outgoing emails. Email encryption dramatically limits the hacker's ability to infiltrate the firm by flagging and quarantining all suspicious communications.