What Regulators Are Looking for in Your Firm's Cybersecurity

July 26, 2015

Based on what we see happening in the RIA industry, we expect 20% of financial advisory firms will have some type of security breach from an outsider this year. With investor protections as their foremost concern, no wonder regulators are asking independent registered investment advisors (RIAs): how ready are you for a security breach?

Cybersecurity readiness encompasses a firm's plan for prevention, investor protection and breach management. At its best, cybersecurity management is a three-legged stool, with equal attention and care given to technology, policies and people for optimal results.
Technology: The Starting Point

Cybersecurity management starts with having the right technology in place to prevent or sidestep disaster. Regulators want to see the kinds of firewall protections RIAs have in place, the usage of passwords and encryption, and whether advisors are using tools like multifactor authentification.
Technologies like firewall hardware and software, antivirus, anti-spam, content filtering, malware software and the like are foundational and mandatory. They identify issues based on what is already known about cybercrime and hacks — including ransomware — and have a huge role to play in prevention.

RIAs should minimize the number of passwords that employees need and consider using password vaults to help them do so. There should be encryption technology in place for email communications and file access. Firms that use cloud-based document vaults for file sharing with clients should take a multi-factor approach by encrypting files prior to putting them in a cloud vault.
Mobile devices used for business purposes, including phones, laptops and tablets, need to be secure and "dumbed down" with limited access points into the firm in the event the device is lost or stolen. The alternative — an older, but nevertheless well-tested option — is to have a policy requiring users to have separate devices for their own personal use, and not for the business of the firm or its clients.

Policies: Managing What You've Got

With the right technologies in place, regulators want to know how RIAs monitor and manage them. Firms need enforceable policies and procedures that reduce the frequency of system issues and improve resiliency when issues do happen.

Good security protocol means backing up the firm's data frequently, and knowing what the data back up to. It means running and reviewing reports and periodically testing backups to

ensure they will work in a crisis.

Technology management and oversight also extends to the firm's external technology providers. According to regulators, RIAs are responsible for knowing what their technology vendors do with their data, and whether their procedures would pass an audit. This includes doing due diligence on the vendor's procedures for keeping the firm's data safe from external breaches and for protecting it from internal sources. For example, what if a vendor encrypts viruses? If the vendor or application provider is doing backups, advisors need to know when the backups are done, who has access and how to get data back should they decide to switch providers.

People: The Weakest Link
The reality is that having technology and corresponding security policies in place is not enough. It is critical that the RIA's people articulate, embrace and practice them. Human awareness is typically the weakest leg of the cybersecurity management stool, and it can cripple the other two legs.

The financial advisory industry generally has a naive attitude about cybersecurity, unaware of the far-reaching impact of its actions. They want to use personal mobile devices for work and vice versa, and can view mandatory passwords, firewalls and the like as obstacles, instead of protections in place for their own benefit. And why not? Anytime, anywhere on-demand access is expected in our society. Without the right training, advisors cannot expect their staff to think differently than anyone else.

RIAs need to provide their staff with awareness training and regularly update and review the firm's security policies. Firms need to bring their technology protocols to life, and monitor to ensure all users comply. Staff also needs to understand the firm's contingency plan in the event of a cybersecurity event or other business disruption, and how this plan is executed.

Advisors may not have the ability or inclination to do all of this internally, so finding a trusted partner (or partners) who understands industry regulations and how they translate into appropriate policies and solutions is key. For example, RIAs may want the help of a compliance officer to develop key documents. They may want objective advice about their technology options, and what makes the most sense for them. The Threat Is Nearer Than You Think

Hackers are looking for big payoffs for little effort, and the financial advisory industry seems to deliver. RIAs in particular can be slower to embrace new technology, have relatively lax cybersecurity policies, and control or have access to large amounts of assets, approaching or passing the billion-dollar mark in many cases.

But security breaches do not always originate from the outside, nor are they always intentional. The U.S. Federal Deposit Insurance Corp. (FDIC) breach happened in 2015 when

an employee downloaded 44,000 files on its bank clients' bankruptcy plans onto a USB thumb drive and then quit. Phishing emails have gotten more sophisticated, and following directives or clicking on links from suspicious emails is still commonplace.

Any simple, unexpected event has the potential to disrupt a firm's business. Human error, a network or computer failure — the internet goes down — can trigger a business disruption that requires a well-thought contingency or security plan to kick into place.

Act Now

It is time for advisors to act against cybersecurity threats for the sake of their clients and for their firms. Wealth management firms are in the crosshairs for cyberthieves, and it is a question of when, not if, firms get hit.

The best approach combines the latest preventive and predictive technologies; well thought, enforced security policies and protocol; and awareness training to foster a sustainable cybersecurity culture in the firm.

RIAs that do nothing — or do not try — will be penalized by regulators. These firms are also leaving doors wide open with welcome mats for hackers and cyberthieves seeking access to client data and assets.