December 8, 2015

No advisor wants to think a cybersecurity breach could happen to them, but ignoring the possibility only increases the risk of exposure. Unfortunately, the registered investment advisor (RIA) industry is a long way away from being ”cybersecure.“ In fact, the SEC’s office of Compliance Inspections and Examinations (OCIE) found in a sweep exam of RIAs that 74 percent had experienced cyberattacks either directly or indirectly through vendors.

Here are seven of the most common mistakes that advisors make when protecting their firms from unwanted cyberattacks and security breaches.

7. Not Budgeting Appropriately For Cybersecurity

Cybersecurity management requires commitment of time and resources. Unfortunately, many advisors fall short when budgeting for cybersecurity, which increases their firm’s exposure to a potential breach. RIA owners need to consider cybersecurity investments as part of their firm’s larger risk management budget, and as an investment in cost avoidance. Experience has shown that for advisors with some security measures already in place, a good rule of thumb is to consider their annual IT budget, and add on an additional 25 percent for cybersecurity protection—i.e., a business class firewall—in addition to ongoing training and policy management.

6. Delegating Full Cybersecurity / IT Oversight To Employees

RIA owners cannot afford to delegate cybersecurity and IT oversight entirely to their firm’s resident technology expert. Cybersecurity threats are increasingly sophisticated, and the regulatory environment is evolving too. Ultimately, it is the RIA owner’s responsibility when something goes wrong, so owners need checks and balances in place for their own protection.

Firm owners need to monitor how their IT policies and procedures are executed, and whether there are any insider leaks. Cybersecurity mistakes happen because of non-adherence to policy and when no one monitors what is happening. RIA owners need to know who is logging in to what, when and where, in the event of a cybersecurity breach. Employees can manage IT issues and functions, but procedures must be documented.

5. Misunderstanding The Virtues Of The Cloud

One of the biggest mistakes advisors make is overestimating the protection offered by the cloud environment. The cloud can generally offer security for data and documents stored within it, though the level and type of encryption varies by provider.

When information is used outside of the cloud, there are no guarantees. RIA owners should be concerned with how, when and where documents are accessed regardless of where they

are stored. Information that is downloaded and used on unsecure, unencrypted devices has the potential to expose the firm to cybersecurity issues once put back to the cloud.

4. Client Service Overrides Client Security

It is natural for advisors to want to help clients with transactional requests that seem to merit an immediate response. But excellent client service also means the RIA has policies that validate these requests to ensure they are legitimate. In its sweep exam of RIAs, OCIE found that almost half reported receiving fraudulent emails seeking to transfer client funds.

Advisors must have procedures for validating email and telephone requests for wire transfers, and for identifying and confirming clients. Clients must also know how the RIA handles these types of inbound requests. For example, a client who has forgotten their account login can be directed to re-register themselves and answer their own security questions, rather than being given a password prompt or other personal information over the telephone.

3. Poor Password Protocol

Password vaults have emerged as a secure solution for RIAs managing multiple passwords from multiple people using multiple applications, but they are only as secure as the utilization policies implemented by the RIA.

Typically, a password vault uses a master password that allows access to all of the pass cards in the vault. Pass cards hold the authentication credentials to access specific applications, and automatically log the user into their assigned applications. If the users are allowed to create their own pass cards, they will also have the credentials to access the applications without the use of the vault, potentially on unprotected or virus-infected devices, increasing the risk of a breach.

It is more effective for the RIAs to have the security administrator or compliance officer create the pass cards for all employees for all business-based applications. This approach should eliminate the possibility that employees have access to core business applications outside of the password vault and secure devices.

2. Lax Enforcement Of Security Policies

Cybersecurity is as much about enforcement as it is about policy. Strong cybersecurity policies will generally address issues related to device usage, user authentication, the Internet, social media and email. Advisors need to reconsider policies that permit personal devices to be used for business purposes. RIA owners must recognize that when its data can be accessed using any unsecure, unprotected device or application, the firm is exposed to real cybersecurity issues.

For example, a RIA may have an encrypted, password protected email system. But once the firm email is synced to an unprotected device, the email become unsecure and the entire firm is now potentially exposed to malware and phishing viruses.

The issue is often not about storing data or email inside the firm. The increased cybersecurity risk can happen when the information leaves the safe environment and ends up on unprotected personal devices and laptops.

1. Low Cybersecurity Awareness

The number one cybersecurity mistake advisors make is to assume that everyone knows what the threats are and how to protect the firm. Unless firm owners are working actively to create a culture of cybersecurity awareness, this is never the case.

RIA owners can elevate the level of cybersecurity awareness in their existing culture by leading through example with ongoing verbal, written and electronic reminders. RIA management should budget time in meetings to address these issues and consider having outside consultants come in for occasional briefings, training or updates.

Where's the data?

Cybersecurity is not something RIAs can afford to address once in a policy handout and never revisit. RIA owners need to keep cybersecurity management at the forefront by continually asking themselves, "Where's the data?" Even if information is safe when stored, and safe in transmission, the firm may still be at risk if its data is being used on unprotected, unsecure devices.

Wes Stillman is CEO of RightSize Solutions, a provider of intelligent cloud technology and business management solutions for advisors. He can be reached at wnstillman@rightsize-solutions.com.