RIGHTSIZE SOLUTIONS

The Cybersecurity Policy Upgrade Imperative for RIAs

The increased reliance on web-based solutions and increased usage of mobile devices means that independent registered investment advisors (RIAs) are at an exponentially greater risk of being cyber attacked than they are of being audited by the U.S. Securities and Exchange Commission (SEC). Unlike a SEC audit, which only a small percentage of RIAs face every year - just 13% of SEC-registered firms in 2017, according to the SEC's FY 2018 Congressional Budget Justification - online attacks occur daily and the scope and severity of these attacks are increasing.

In fact, cyber criminals have become more astute at flying under the radar. Successful security breaches are increasingly subtle and do not disrupt RIA operations immediately, many times it is only after a client is missing assets that firms realize they have been attacked.

SEC Regulation S-P requires RIAs to adopt written policies and procedures governing safeguard for the protection of customer information and records. These policies and procedures must:

- **Ensure the security and confidentiality of customer records and information**
- **Protect against anticipated threats or hazards to the security or integrity of customer records and information**
- **Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer**

Similarly, Regulation S-ID requires RIAs to establish programs that address how to identify, detect and respond to potential identity theft red flags.

The SEC has made clear that cybersecurity protection measures at RIA firms are in need of an overhaul. In fact, the August 7, 2017, alert from its Office of Compliance Inspections and Examinations (OCIE) is candid about the extent to which firms are falling short on planning and implementing meaningful cybersecurity risk policies. The report points out that while most RIAs may be "checking the box" in terms of having written cybersecurity policies and procedures on hand, what is on file is either woefully inadequate or not being implemented, or both.

It's true that RIAs need cybersecurity policies that will satisfy regulators in the event of an audit or investigation. But focusing solely on compliance misses the mark: the most compelling reason for RIAs to implement ironclad policies is to survive cybersecurity attacks and protect firm and client data.

Frankly, just like building a house without a blueprint plan, it is thoughtless for RIAs to attempt to implement technology or cybersecurity measures without a policy. Even though RIAs will not be able to thwart all potential cyber risks, firms are still on the hook for building out policies and procedures with robust controls. From risk assessment and prevention, mitigation, resilience and recovery, a cybersecurity policy exists to give the RIA a framework for dealing with the lifecycle of perceived threats. After all, it is impossible to monitor what you cannot measure.

The OCIE report points to six areas that RIAs need to focus on for their written cybersecurity policies that document enforceable procedures:

1. **GOVERNANCE AND RISK ASSESSMENT.** Firms need to map out how they will make decisions and handle issues related to cybersecurity intrusions. This includes a framework for conducting regular assessments and inventories of data, software, hardware and vendors to identify vulnerabilities, classifying their threat level and implementing a process for remediation.

2. **ACCESS RIGHTS AND CONTROLS.** RIAs are expected to establish and enforce access controls to data and systems. This means protecting information in all of its forms from misuse, theft, unauthorized dissemination, manipulation and destruction. The protection may be either physical or software-based.

3. **DATA LOSS PREVENTION.** These policies are meant to protect against the unauthorized transfer of information within and outside of a firm. RIAs must monitor the content transferred outside of the firm by its employees or through third parties, including email attachments or uploads. Firms must also monitor for unauthorized data transfers and must have procedures in place to verify the authenticity of client requests to transfer funds.

4. **VENDOR MANAGEMENT.** If not managed correctly, third-party service providers may expose RIAs and their clients to cybersecurity risks. Firms should have risk-management policies and procedures for sharing private, confidential and / or internal information with outside vendors and service providers.

5. **TRAINING.** RIAs should require mandatory information security training for all staff as part of their on-boarding process. Firms should also provide additional training periodically and as needed, particularly in response to newly identified risks, operational changes, new regulatory requirements or the firm's experiences with cybersecurity threats. Firms should document that employees have completed the required training.

6. **INCIDENT RESPONSE.** RIAs should have documented, written procedures for responding to and reporting incidents involving unauthorized access to, or unauthorized disclosure or use of, personal information. In so doing, firms will need to also adhere to their state's security breach incident reporting requirements.

Though all of these areas need to be addressed in a cybersecurity policy, there is no such thing as a one-size-fits-all solution. Each RIA is unique in its business operations, strategy and client mix, and likewise each firm's policy and procedures should be thoughtfully constructed to meet their specific cybersecurity needs.

SENIOR LEADERSHIP ON CYBERSECURITY

For a cybersecurity policy to function as it should, it requires oversight from the most senior levels of the RIA management team. In fact, SEC chairman Jay Clayton noted in his September 20, 2017, statement on cybersecurity, "It is our experience…that a focus by senior management on cybersecurity is an important contributor to the effective identification and mitigation of cybersecurity risks."

Simply put, the firm's Chief Information Officer / Chief Information Security Officer must be someone who understands what the potential cybersecurity risks are to the business as a whole, and who has the authority to act. Delegating cybersecurity issues to a mid or junior-level staffer only dilutes the effectiveness of the firm's policy and procedures, no matter how stringent they may seem on paper. It is less important that this C-level executive be a technology expert, and more important that they

be disciplined and have the necessary gravitas to enforce a culture of compliance. The cybersecurity policy and procedures will only be as effective as the level of authority the firm puts behind it.

SPOTLIGHT ON DATA LOSS PREVENTION: EMAIL

Email is a primary means for RIA communication with clients, vendors, other third parties and within the firm. As a result, most breaches happen through email, due to some combination of user error and gaps in cybersecurity protection. An integral part of daily RIA operations, the consequences of email misuse and fraud can be devastating.

For example, client email accounts are prime targets for identity thieves, who send bogus emails from hacked accounts. “Spoofed emails” are used to transfer money successfully from investment accounts from unsuspecting RIAs.

A spoofed email address is a fraudulent email account that looks similar enough to a legitimate email address so to appear correct to the unsuspecting receiver, who may not recognize innocuous differences - e.g., changed domain name from .com to .net, or adding, removing or substituting a character from the correct address.

If these mistakes were typed in unintentionally, email to this address would bounce back as incorrect. However, a “spoofed” email is tied an actual account that has been set up by the criminal with an address that closely resembles one that the end receiver would recognize. When the recipient replies to the email, they correspond directly with the thief without realizing it.

Correct:	wstillman@rightsize-solutions.com	
Spoofed:	wstillman@rightsize-solutions.net	spoof: “.net” extension
	wstilman@rightsize-solutions.com	spoof: missing “l” in stillman
	wstillman@rightsizesolutions.com	spoof: missing hyphen between “rightsize-solutions”

Consider: Using a spoofed email address, a thief gets in touch with a financial advisor posing as an existing client to request an update on an account balance. In his reply email, the advisor gives the account balance, which prompts the thief to request a wire transfer. The wire transfer request also includes an excuse from the thief for why they cannot be reached via telephone to validate their identity – typically an illness or death in the family prevents them from conducting business as usual. The advisor accepts the rationale and executes the wire transfer of funds out of their client’s account and into that of the thief.

This chain of events is the result of a sophisticated criminal or criminal network that has broken into the client’s personal email account at some point in the past. They have spent time monitoring their email usage and communication patterns. The cybertheives have gotten to know who this individual corresponds with and where the potential assets are. They can also adopt the individual’s communication style well enough to commit a crime.

EMAIL HACKS CAN HAPPEN TO RIAS, TOO

Without an enforced cybersecurity policy that includes user authentication protocols and network security to prevent unauthorized access to a firm’s private network, RIAs are as vulnerable to spoofing and email hacks as their clients. Typically, an unsuspecting advisor or firm employee will click on a link inside a phishing email, which immediately compromises the account.

Once the account has been hacked, the thief can send emails that are legitimately from the advisor’s account. They also have access to everything, not just email. This means the thief can tap into client emails and nonpublic client information, and communicate directly with clients using the advisor’s legitimate email address.

To avoid getting caught by the RIA, which would happen when a client replied to an email, the thief initiates auto-forwarding rules for the advisor's email account, so that communications circumvent the advisor's inbox and are passed to the thief.

AN OUNCE OF PREVENTION

A strong cybersecurity policy will mandate the firm have conditional access rules and technology in place to help prevent these issues, including multi-factor authentication (MFA) and email monitoring.

Conditional access rules help verify the user and help prevent unauthorized access to the firm's private resources. To gain access, users must log in with strong passwords from a registered and secured device - or from any device, via their private cloud environment.

RIAs should have protocols to routinely watch email rules to make sure that nothing is being forwarded automatically outside the firm. As an added layer of protection, RIAs should prohibit personnel from accessing their personal email accounts through the firm's private network.

For inbound emails, protocols can alert advisors to the potential of fraud and thwart criminal attempts to access client accounts and personal information. This can include staff training, mandatory verbal confirmations of transfer requests, and client email prompts. RIAs can also mandate encryption on emails that are flagged as containing personally identifiable or sensitive information, or use portals or shared folders for transmitting this type of data.

THE CYBERSECURITY IMPERATIVE

The internet and electronic communications are integral to how RIAs do business and interact with clients, making the cybersecurity policy a necessary defense against bad actors. The majority of cyber events are caused by carelessness, ill-will or lack of training, but malicious attacks can come from anywhere. This includes external cybercriminals and hacktivists, competitors, vendors, and even firm insiders or employees.

Unfortunately, most RIAs lack a workable cybersecurity policy because they do not know how or where to begin. This makes them easy targets in an age where cybercriminals are running highly sophisticated and highly lucrative operations. Without a multi-faceted program in place, cybersecurity becomes a game of whac-a-mole, and RIAs simply do not stand a chance.

What RIA owners can do, is put in place the best tools and continually improve their firm's security. By weaving cybersecurity protocols into the fabric of daily operations, the policy protects and monitors access, data storage and transmission from the RIA perspective.

In fact, a best-in-class cybersecurity policy can enhance the overall client experience, which can be a differentiator as concerns over security issues continue to grow. Managed with the right partner, an enforceable policy ultimately benefits everyone – RIA owners, staff, and clients – and allows advisors to focus on doing what they do best.

14425 College Boulevard, Suite 150
Lenexa, Kansas 66215
(913) 396-4600
info@rightsize-solutions.com

RIGHTSIZE SOLUTIONS