RIGHTSIZE SOLUTIONS

Changing the Cybersecurity Conversation

How RIAs can positively respond to the call of cybersecurity within all aspects of their business; firm culture, client experience, operational management, and business development.

Overview

The overwhelming amount of daily news stories on data breaches, ransomware attacks, malware and viruses remind us daily that cybersecurity is, and will continue to be, prominent in our personal and business lives. This fact puts RIAs in a precarious position as they're responsible for both the security of their own firm and that of the personal data of their clients.

This news is often delivered in a piece meal format in bite-size articles. While this steady drip is a constant reminder of the increasing risk, it does not provide answers on how to prevent attacks, where to start first, and how to bolster defenses for the long run. News stories fail to recommend that your approach towards managing your firm's cybersecurity should be a holistic and comprehensive idea. It's no longer an option to view cybersecurity as just a component of your overall technology plan. RIAs need to use proper cybersecurity as an overarching framework to plan, manage and budget all IT initiatives. Small RIAs are more susceptible to cyberattacks than their owners would like to believe. In fact, with smaller technology budgets and insufficient controls, small firms may be the perfect targets for hackers. Implementing and enforcing cybersecurity measures properly doesn't have to break the bank though. Even without deep pockets to invest in cybersecurity, RIAs need to have policies and measures in place to prevent fraud.

While media coverage of cyber incidents has built well-deserved awareness, it has done little to provide answers, and instead has generated only fear. As a managed security service provider, RightSize Solutions has every reason to reinforce caution and focus on the consequences of an inadequate cyber-policy, but in this whitepaper we'll take a slightly different approach; demonstrating how to deal with cybersecurity in a proactive and positive way that can significantly contribute to the growth of your firm.

As public awareness of high-profile breaches continues to grow, advisors should put themselves in a position to confidently answer the questions of apprehensive prospects and clients. By better implementing cybersecurity education, policies & procedures, and best practices, RIAs can provide a differentiated service to their clients that directly addresses one of investors' fastest growing concerns.

Changing the Cybersecurity Conversation

Cybersecurity is the mission focused and risk optimized management of information which maximizes confidentiality, integrity, and availability using a balanced mix of people, policy and technology while perennially improving over time."

- Dr. Mansur, Global Cybersecurity Thought Leader

1. Knowledge is Power

Ways to empower staff to enhance the client experience

Policies and Procedures are only as good as your weakest link. Learn how to empower employees to recognize red flags and confidently respond to potential incidents. Basic education can go a long way toward increasing client service efficiency and productivity.

Encourage your employees to report abnormalities, and avoid discouraging false alarms. Building an environment where employees feel comfortable reporting issues without repercussions is paramount to identifying and acting upon breaches or other cyber issues as soon as possible. While first instinct might be to chastise an employee that opened a questionable email attachment, being able to act in the first couple hours can actually save a lot of damage. You will be much worse off if the employee doesn't report it, and the virus/ransomware/malware, is able to run for hours, days, even months without detection.

The Pew Research Center offers a **Cybersecurity Knowledge Quiz** to test your knowledge on cybersecurity topics and terms by taking their 10-question quiz. When you finish, you will be able to compare your scores with the average American and see explanations for the terms and topics in each question.

For more information, read our Tech Trends blog:

Tales from the Frontline: A Thwarted Phishing Attempt

How to Handle Employees Leaving…

Back to the Basics

Think back to grammar school and the importance of the fire drill. Many industries use drills as a regular practice; from police and fire departments to retail stores preparing for Black Friday.

Schedule a cyber-awareness day or education workshops that simulate what attacks on employees would look like. During downtime, have employees or interns simulate phishing attacks; both emails and phone calls. There is a cottage industry of training firms that create learning experiences to reward those who react favorably and coach employees who fall to the simulation. And don't forget the obvious. Be sure to check your entire office and work space for physical vulnerability violations such as sticky notes on monitors. Hiring a third-party firm to audit your security policies and enforcement procedures, perform a network assessment, and test vulnerability of your systems may prove to be one of the best investments you have ever made.

"If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked"

- Richard Clarke, Former National Coordinator for Security, Infrastructure Protection and Counter-terrorism

2. 

Check Under the Hood
Examining infrastructure and service provider solutions

Is your IT environment optimized for your individual business? The RIA industry is comprised of many small businesses with wildly different operating models. Understanding the different management approaches will help you make more informed, and ultimately better, decisions when evaluating the service-provider-solutions.

Evaluating the IT Environment Options

At the high level, infrastructure can be either centralized or decentralized. Decentralized environments, where each function and application is managed independently and directly with vendors, are often considered easier to implement and work well for small firms where accountability is easily measured. Alternatively, centralized environments generally take more effort to establish, but offer heightened security measures, and a secure way to scale businesses. Centralized environments consolidate the core business applications and data into a single system for ease of management and auditing. A centralized environment is typically maintained by a managed service provider.

For example, in a decentralized environment, an advisor might have the freedom to access their portfolio management system from any device anywhere in the world. On the other hand, a centralized environment can provide many of the same freedoms, but might require an extra step of security, like logging into a secure network through a VPN, or only being able to access data and applications from a short list of registered devices.

Either environment can work securely and safely, but it's up to the advisor to determine the right fit, either through their own effort or with the help of a managed security service provider. In some cases, RIAs might find it within their best interest to pursue a hybrid solution that requires stricter security measures for employees that would only ever need to access data while in the office, and allows greater mobility to employees that might be traveling for business to meet with clients.

Whether you're starting a new Registered Investment Advisor (RIA) or are an established firm looking to make improvements, deciding how to manage technology can be one of the most important decisions you make. Make sure the firms that support you are backing up their security claims with trustworthy actions.

Vendor Due Diligence

Once you've established the type of environment that best fits your needs, it's time to move on to deciding on the vendor to engage with. Here are 7 essential questions you should know the answers to, before deciding on a technology or any other service provider.

Changing the Cybersecurity Conversation

1. **How do they rate?** What is the firm's Net Promoter Score? What is the client retention rate? Always ask for client references that you can interview for their experience. Your technology partners - for better or worse - are an extension of your brand. And so, it is critical that you are philosophically aligned with your approach to client service. A Net Promoter Score is a clear proof-point to confirm that alignment.

2. **What are the firm's policies and procedures?** If a firm is going to support your infrastructure, you should be sure the firm has undergone intensive due diligence, including areas such as private client vulnerability testing. Technology service providers - especially Managed Security Service Providers (MSP) who are "partners" in your business - are well positioned to contribute to your firm's policies and procedures and otherwise make sure yours will stand up to auditor reviews.

3. **How do they invest in technology?** Simply put, be sure they have a strong research and development team and utilize the most cutting-edge software and hardware for their customers. Also, the service provider's experience specifically in the wealth management and RIA industry can be invaluable. This will help with not only insuring a smooth implementation but also how well they will respond to any questions or potential problems as they arise.

4. **Who are their vendors?** Technology vendors will have vendors of their own. It is absolutely within your right to ask for details on what services they use, and what policies they uphold in the management of those relationships. While a few degrees of separation away from your advisor business, a vendor's reliance on Amazon Web Services, Microsoft Azure, IBM, Google, or other providers could affect your business. This past summer, an elections analytics company left data of 198 million US voters publicly accessible, simply by improperly configuring their data repository with Amazon Web Services.

5. **Are services fees all-inclusive or a la carte?** The old adage 'you get what you pay for' is especially true with technology. The better service providers are not out to nickel-and-dime you. Understand the fee structure before you sign on the dotted line. Service providers who are willing to make the investment in time to understanding your specific needs and goals in the early stages are typically thorough in the process of preparing a client to adequately utilize the technology.

6. **Who will be supporting you?** You are available as a trusted partner to your clients - so should your services providers be to you. You most likely are hiring them based on industry experience and expertise. Make sure you have access to staff at all levels of the organization.

7. **What are the guarantees?** While there are no guarantees in life, there are when it comes to services and products. Understand how a service provider stands behind their work. You don't need to be a lawyer to know that most service level agreements (SLAs) favor the vendor not the clients. Know what you're getting into before you make any long-term commitments. Especially with those just getting started, there will always be unforeseen situations that can delay your start date. An SLA may impact your bottom line by demanding you pay for services you may not need right away.

For more information on what a cybersecurity focused technology environment should cost, read our article from Financial Planning: *How much does cybersecurity cost?*

Read our Tech Trends blog: *Are you making employees handle IT?*

"We need a cybersecurity renaissance in this Country that promotes cyber hygiene and a security centric corporate culture applied and continuously reinforced by peer pressure"

- James Scott, Author, The CEO's Manual On Cyber Security

3. Measuring Cybersecurity at All Levels of the Organization

While cybersecurity is typically viewed as a function of operations, it can also contribute to the growth and success of your firm. Discover ways to leverage this advantage when communicating with colleagues and business partners.

A recent CIO article explains how technology touches all employees within an organization, not just those in the IT department. A commitment to proper technology management will permeate from the top on down. Set this precedent by establishing the following ideas:

- **Establish the right metrics:** Access Control and DLP must be a holistic approach Remember that third parties only control what is in their environment not the devices accessing their system. I think we need to make a clear point that the actual access to cloud based applications is Just as important if not maybe more so than protecting the data once it is in a third party's control.

- **Unite business and technology processes:** Elevating cybersecurity to a department-agnostic issue goes beyond deploying data loss prevention or identity access management solutions. It involves formalizing new processes (and updating existing ones) through a combined business and IT lens. Risk and compliance management, new vendor selection and end user security training can't be practices that IT departments outline and impose on their colleagues. All business leaders must be equally involved in shaping these policies to ensure they are enforced and effective.

- **Promote a new outlook for security spending:** Security comprises a single slice of the IT budget, historically viewed as something to be contained, and requiring investment only in times of real or looming crisis. Organizations striving to foster a culture of security need more proactive stances toward their strategy and spending. This means positioning cybersecurity as an investment opportunity, not a reluctant line item.

- **Make Contingency Plans.** In addition to drills and quizzes, you should also have a cybersecurity communications plan in place for media, customers, partners, and shareholders. Prepare email communications, press releases, and landing pages to explain what happened, how your company is addressing it, and what customers should do in the meantime. This practice shouldn't be reserved solely for cyber-events. Firms should have communication and action plans in place for other events that might hamper day-to-day operations like natural disasters.

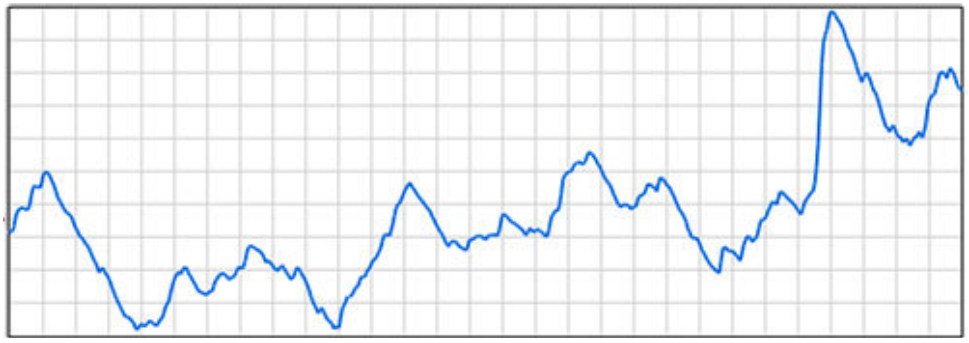
"One of the main cyber-risks is to think they don't exist. The other is to try to treat all potential risks. Fix the basics, protect first what matters for your business and be ready to react properly to pertinent threats. Think data, but also business services integrity, awareness, customer experience, compliance, and reputation."

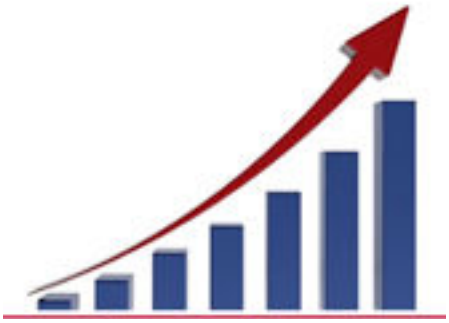
- Stephane Nappo, Global Chief Information Security Officer & Board advisor, Société Générale

4. The Human Element

How to shift the conversation from fear to enlightenment

How you speak about cybersecurity is as important as how well you actually manage it. While formalizing an actual cybersecurity plan is essential, it's only as good as the people who are managing to that plan. As an advisor to your client's finances, one of your responsibilities is to educate and enlighten them that they have more power than they're aware of. The same is true when it comes to cybersecurity. Knowledge is power and it is your responsibility to continually educate your staff, clients, and partners.





The barrage of daily news can cause anxiety for the calmest among us.
Change the lens to view these interruptions with the confidence that you've got this covered.

The grid below provides practical steps that your employee and clients should take for the protection and safety of the firms and data.

Control	Best Practice
Use secure passwords	Remind associates to use secure passwords and multi factor authentication. These days, passwords are quickly becoming just a part of confirming identity. Having a combination of a password and a personal identifier (something you know, and something you have) is quickly becoming the norm.
Use a password manager	Password managers provide access across multiple devices, programs, and apps. Opt for the premium or enterprise version to receive extra features, such as alerts when one of your sites or services has been breached and priority customer service.

Changing the Cybersecurity Conversation

Control	Best Practice
Encrypt your devices	Encryption technology can be cumbersome and relatively time consuming compared to typical online interaction but has a very real and important business purpose. Recognize when it's appropriate and don't overuse encryption. Sending encrypted emails for basic email communication will quickly become tiresome for your employees and clients, but when used properly can help PII and PFI from leaking.
Be suspicious - learn to identify phishing emails	Be on alert for the red flags, such as emails that ask for personal or credit card information, requests for immediate action regarding unfamiliar situations, or emails that include suspicious attachments.
Keep an eye on the news for security incidents	You can quickly be overwhelmed by the news of the day. Relay on trusted industry sources, service partners, and regulatory organizations to avoid unnecessary noise and for better clarity on what matter most to you.
Back up your data	Backups must be designed to support the everyday mishaps of accidental file deletions as well as both minor and major disasters. Local backups provide fast access for recovery but are vulnerable to hardware and environmental failures. Remote or off-site backups solves the issues of local backups and can provide a robust, economical solutions, but require time for restoration. Implement a strategy that focuses on what must be recovered first, and how long it will take to get you back and up and running.
Keep software, programs, and applications up to date	Not only will you be more secure but will also perform better and be more reliable. Include scheduling regular downloads of security updates, which help guard against new viruses and variations of old threats.
Use a Business class router/firewall	A firewall prevents unauthorized access to or from a private network and can be implemented as both hardware and software, or a combination of both. In essence, a firewall examines each message and blocks those that do not meet the specified security criteria. Also, take the extra precaution to go beyond just the one provided by your ISP.
Secure your Wi-Fi	Your wireless router is a prime target for hackers wanting to infiltrate your network or freeload off your Wi-Fi connection. Periodically changing passwords and checking your router settings is a good practice.

Changing the Cybersecurity Conversation

Control	Best Practice
Understand the importance and nuances of data loss prevention	How is your firm monitoring the volume of content transferred outside of the firm by its employees or through third parties, such as by email attachments or upload? This includes how your firm monitors for potentially unauthorized data transfers and may review how firms verify the authenticity of a customer request to transfer funds.
Use an alternate checking account for all Online Bill Pay and ATM transactions	Do not respond to or send any information to any bill pay service that asks for personal or financial information directly through email. Email is a notoriously insecure form of communication, and reputable services will never request sensitive personal or financial information through email.
Restricting TMI- limiting the amount of personal information you post online	This is another common sense one. Restricting Too Much Information (TMI) can save you from identity theft and even protect your physical safety. Never share your social security number (including even just the last 4 digits), your birth date, home address or home phone number). Social networking sites increasingly give users more control over customizing the privacy settings. Don't assume you have to take whatever default settings the site gives you.
Disable Cookies	In addition to providing privacy, it will free up space on your computer hard drive. Another option is using DuckDuckGo, a search engine browser that doesn't track you and protects your search history.
Do not use Public WiFi	Falling victim to public Wi-Fi's dangers is a question of when, not if. Convenience seems to outweigh consequence, especially with how people use their mobile devices. However, using free public Wi-Fi comes with any number of serious security risks. Make the investment of an unlimited data plan for your device for the best solution here.
Stop Playing Games on the internet or downloading them on your business computer	Folks, does this one really need an explanation…

Changing the Cybersecurity Conversation

With all the effort you're now putting into cyber security, make sure you dedicate space on your public facing materials, such as your website and ADV, to let existing and prospective clients know how you proactively manage cybersecurity. As an example, Brad Ferguson, chief investment strategist for Investment Management at Halter Ferguson Financial created this blog post:

RIA Cybersecurity - Your Security is Our Priority

Client Testimonial:

> *Safety and less downtime were the main reasons we engaged the services of RightSize Solutions. The Kansas City-based firm specializes in RIA cybersecurity and offers a "cloud-based" platform. Cloud-based services are becoming more and more common. If you have an iPhone or iPad, you are probably familiar with Apple's iCloud, a way to back up your electronic data. What it means for us is our desktop, documents, and programs are not housed on the machine in front of us. We access these via the internet. Their service is supported by a U.S. based help desk, staffed 24/7.*
>
> *What this means is our physical computers are still present, but we now use them differently. When we log onto our computer, we click an icon that takes us into a virtual environment. A desktop within our desktop. The computer we work on is in Kansas City. Secured and monitored off-site and guarded with military grade RIA cybersecurity technology. Read the entire article: 6 steps to creating a culture of security ownership.*

For more information, read our Tech Trends blog 5 Key Questions RIAs Should Ask This Month.

Conclusion:

'Changing the Cybersecurity Conversation' is not easy and is an ongoing process. However, just as you advise clients to focus on the whole picture and the long term financial future, you need to take the same approach towards cybersecurity. Just as there will be daily ups and down in the market, there will be ups and downs with security and technology risks. 'Past performance does not necessarily predict future results' rings true here too. Ultimately, your responsibility is to establish a holistic and comprehensive solution that best addresses all aspects of cybersecurity to provide the peace of mind that allows you to not be distracted by all the noise, so you can focus on running your business as efficiently and productively as possible.

About the Author

Wes Stillman is the CEO of RightSize Solutions, a premiere provider of outsourced IT. Wes launched RightSize Solutions in 2002 to respond to RIAs that needed a technology partner who truely understood their business. RightSize Solutions has since grown to provide a full service IT solution that helps advisors of all types and sizes to expand and protect their businesses. A technology-pioneer in every sense, Wes is regularly quoted as a subject matter expert in industry publications and also speaks to small and large groups on topics such as cybersecurity, cloud-based environments and leveraging technology

About RightSize Solutions

RightSize Solutions is a privately held company headquartered in Overland Park, KS. Our company roots date back to 2002 and our focus is exclusively in the registered investment advisor (RIA) community. As the premier provider of IT Management Services for the wealth management community, we are proud of our heritage which includes being the very first provider of outsourced technology management and Cloudbased cybersecurity solutions to RIAs.

We provide all prospective clients with a full technology assessment of their network. Have existing tech problems? Our support team would love a chance to demonstrate their knowledge. At no cost to you

Call (913) 396-4600 or email us at info@rightsize-solutions.com.

Technology assessment includes:

- Free 45 minute consultation (a $500 value)
- Complete assessment of technology environment

Subscribe to our newsletter

- Sign up at rightsize-solutions.com
- Monthly blog posts, articles and Cybersecurity News Commentary

11011 King Street, Suite 280
Overland Park, KS 66210
(913) 396-4600
info@rightsize-solutions.com

RIGHTSIZE SOLUTIONS

RIGHTSIZE
SOLUTIONS