WHITEPAPER

7 CYBER SECURITY AND COMPLIANCE FOUNDATIONS FOR RIAs

Introduction

Cyber security defense should be a top priority for every Registered Investment Adviser (RIA). The reasons are two fold.

Despite the conventional wisdom, smaller firms are just as likely to fall prey to cyber criminals as larger enterprises.

First, most RIA firms are small businesses with less 100 employees. Despite the conventional wisdom, smaller firms are just as likely to fall prey to cyber criminals as larger enterprises. In a recent cyber security research report published by Verizon, 10% of data breaches impacted firms in the financial sector overall and 43% of those attacks hit small businesses, defined as firms with less than 100 employees.[1] Unfortunately, smaller firms also often lack the budgets and sophisticated cyber security tools of larger enterprises. Nevertheless, the stakes are just as high. All RIAs, no matter the size, run the risk of disruptive ransomware attacks, data and intellectual property theft, damage or abuse by disgruntled employees, or financial fraud.

[1] Verizon: 2019 Data Breach Investigations Report

In this whitepaper, we will share the seven most important cyber security and compliance foundations for RIAs.

What is the OCIE?

Just as importantly, all RIA firms are also regulated the Securities and Exchange Commission (SEC) and its inspection arm Office of Compliance Inspections and Examinations (OCIE). The OCIE's mission is to protect investors, ensure market integrity and support responsible capital formation through risk-focused strategies that: (1) improve compliance; (2) prevent fraud; (3) monitor risk; and (4) inform policy.[2] RIAs are considered "covered entities" by the SEC just like larger broker dealers and are subject to the broad compliance requirements and regular inspection by the OCIE.

Cyber security safeguards are a key component in protecting investors from fraud and cyber crime. Since 2015, the OCIE has consistently identified cyber security among the agency's top focus areas. On average, it is likely most first RIA firms will be subject to an OCIE inspection at least once over a six year period. Therefore, RIA firms have a clear compliance and business need to consistently invest in cyber security and ongoing risk management.

Getting Started, Staying Compliant

Unfortunately for many firms, it is likely confusing and overwhelming to assess your current level of compliance in the cyber security arena. The purpose of this whitepaper is to provide a road map for how to take stock of your current level of compliance and readiness and where to go next. In this whitepaper, we will share the seven most important cyber security and compliance foundations for RIAs.

[2] https://www.sec.gov/ocie

Choose a cyber security standard

1

There are several different cyber security standards available from government agencies and industry bodies. A cyber security standard is vital for helping organizations identify gaps and risks and to benchmark themselves. At its most basic level, a standard is a checklist of must-have capabilities, resources, and procedures that an organization must have in place for sound cyber security. Standards also are critical tools in doing a thorough risk assessment.

There are several good cyber security standards available:

- International Organization for Standardization (ISO) **ISO/IEC 27032:2012**
- Center for Internet Security (**CIS**)
- Control Objectives for Information and Related Technology **(COBIT) 2019**
- National Institute of Standards and Technology **(NIST) Cyber Security Framework**

There are a few different reasons itSynergy recommends the NIST Cyber Security Framework (NIST CSF).

First, NIST is an agency of the federal government. NIST is effectively the federal government's science and technology department. So, anything scientific or technology-related comes out of NIST. One of the main things NIST does is to identify the best practices that both government and industry should utilize in a particular area. Since NIST is part of federal government, there will be longevity and continuity with the standard.

The NIST CSF is also referenced by the OCIE as their starting point for all of their cyber security compliance audits. The OCIE specifically mentions the NIST CSF in the footnotes of their annual guidelines. Therefore, when an inspector from the OCIE conducts an investigation, they are going to align first and foremost with the NIST CSF standard.
At the end of the day, the most important step is to pick a standard and actually assess your risks based on the standard and then prioritize your efforts accordingly.

A few years back, NIST published the Cyber Security Framework. It is a very thorough and broadly adopted standard. It is now in its 11th version. The NIST CSF defines five of what they call "functions," and then each function has categories. So there are total of 23 categories and then each category has sub-categories, so in total there are 100 subcategories. The result is a highly detailed 55-page document covering every imaginable dimension to an organization's cyber security. You can also view the standard as a spreadsheet and it is over 500 rows long.

The most important step is to pick a standard and actually assess your risks based on the standard and then prioritize your efforts accordingly.

Start with a risk assessment

The next most important step for RIAs is to conduct a thorough risk assessment of your business. The purpose of assessing risk is to ensure business leaders are fully informed of the level of risk in their organization, to identify mitigation strategies and associated costs for each risk, and to then make informed decisions about the best strategy to create a balance between minimized risk and resource (time, money, usability) utilization.

itSynergy has developed a proprietary model, which we call risk-informed decision-making (RIDM). The idea behind RIDM is that if you are making decisions about technology investments and priorities without having first done a risk assessment, you're wasting your money. The goal of technology and security investments is to get a return on investment (ROI). In our view, before you start to make decisions about where you're going to spend dollars, you need to have a comprehensive risk assessment to help you prioritize those decisions and make sure that you're getting the most bang for your buck.

In short, itSynergy analyzes a client's security posture to each line item in the NIST CSF. We work with the client to understand the probability of a particular security incident or event. For instance, an Internet outage is one particular line item from the NIST CSF. The probability of such an event will be based upon whether the client has a single Internet connection or alternatively, redundant Internet access from diverse providers, configured in an active-active fail over configuration. A score from one to ten is determined for the probability of a specific event. A client with dual Internet access connections may have a probability score of a 2 for any sort of outage; that is, it is highly unlikely to occur. The next step in the process is to determine the impact of a particular event. For instance, if the client leverages lots of cloud applications in their operations, the business impact of an Internet outage would be quite high. In this case, we might give the impact score a seven, on a ten point scale.

Next, we multiply the probability score by the impact score to arrive at the exposure score. These exposure scores are then mapped to a scatter graph, to arrive at a graphical representation of the different risk exposure scores. With the graphical approach, high priority items are identified and are then fed into the strategic planning process of the client.

At this point, a few additional reminders are in order. It is vital to document all assumptions throughout the risk assessment process. These assumptions capture the logic of a particular score. This level of detail is vital for planning purposes and handy in the context of an OCIE compliance audit. Implicit in this process is the idea that not every risk or threat needs to be mitigated at day one. Resources of time and money are limited. And it is perfectly acceptable to prioritize an item as low, if it has a low exposure score. By the same token, it is perfectly acceptable to prioritize and plan for upgrades to mitigate a medium-sized risk at date in the future when resources and budgets will be available. The important part is to document assumptions clearly.

2

To learn more about the itSynergy risk assessment process, visit:

www.itsynergy.com/risk

The purpose of assessing risk is to ensure business leaders are fully informed of the level of risk in their organization.

Security and compliance is a journey, not a destination

3

Cyber security and compliance is an ongoing journey and discipline, but there is no fixed destination or end point.

For instance, a good cyber security risk assessment should be revisited on an annual basis and incorporated into an IT strategic planning process. itSynergy conducts cyber security risk assessments for all new clients and revisits the assessment for each client on at least an annual basis. Risk management realities will change over time, especially as a business grows and becomes more complex. Moreover, the external threat environment is constantly changing as well, increasing or decreasing the probability of certain events. The key reality is that risk management is an ongoing and dynamic process, which needs continual monitoring and engagement by highly trained cyber security professionals, along with sustained engagement of executive leadership of a company.

Thorough record keeping is vital to maintain compliance. The OCIE will want thorough records of changes to the risk management assumptions. As we have noted in the context of the itSynergy risk assessment process, all assumptions are thoroughly documented in the spreadsheet used the in process. Moreover, all documents used in the process are stored in a Microsoft® SharePoint® shared document repository. With SharePoint, all dates and changes are tracked automatically. Document versioning is automatic and there is a built paper trail to track changes to risk assumptions and models.

When an OCIE investigator wants to dig deeply on any cyber security related topic, it is vital to have change management and logging built into your process. The OCIE investigators will want to see a proactive process of ongoing risk management, thorough documentation, and a continuous process of improvement in the security posture of the RIA firm under inspection.

The OCIE wants to see an annual review and change log on every document, not just the risk assessment. Any changes to any of the compliance points should be tracked and documented, and if there are no changes, it should be documented that it was reviewed and decided no changes were made. This is especially applicable to written policies. Even if they aren't changed, the OCIE will want to see you reviewed it, considered changes, and decided not to change anything, along with the appropriate reasoning.

This means that it is vital to budget appropriately for ongoing security investments and to follow through on upgrades and proactive changes to technologies, policies, procedures, and processes. For instance, there may be fairly substantial security investments required from one year to the next, because changes in the firm or the risk environment. It is a very serious problem, if risks are identified, investments are postponed arbitrarily, and the can gets kicked down the road.

An IT service provider partner, like itSynergy, is vital in helping firms handle the changing risk management environment and to follow through in a disciplined fashion with upgrades and improvements.

itSynergy conducts cyber security risk assessments for all new clients and revisits the assessment for each client on at least an annual basis.

Cyber Security Training for everyone on staff

4

The next major investment is proper cyber security training at all levels of an organization.

It cannot be repeated enough, people are the weakest link in cyber security. You can have the most expensive firewall, the most robust intrusion detection system, and the most thorough authentication process in place, and people's bad habits and sloppy behaviors can nevertheless lead to massive security incidents.

Therefore, we need to build a "human firewall," by training people at all levels in an organization, cultivating a culture of security, and ensuring personal discipline by each and every employee.

It is vital to have a tiered approach to training. For instance, IT staff must leverage regular and intensive cyber security training to stay up on the latest trends and changing best practices for professionals and practitioners. Training and learning outcomes should be tested and certified. Executives and other high level staff who handle sensitive internal information, such as financials, intellectual property, or trade secrets will also require specialized training on software and security tools. This sort of training should embrace adult learning best practices and have lots of opportunities for hands-on education.

And lastly, there should be an ongoing and regular cyber security awareness training program designed for all staff. At all levels of the organization, training must be delivered and embraced. Importantly, the training should be deployed in a manner where there is frequency and repetition of the key messages and best practices. Research has shown that annual security training is highly ineffective. Instead, ongoing and online training exercises delivered in bite size chunks, keeps cyber security awareness top of mind and increases compliance and employee engagement.

A cyber security awareness program or service is best paired with mechanisms to test and validate the effectiveness of the training. For instance, most of the best training services deliver simulated phishing email tests to users to determine employee effectiveness at spotting fraudulent emails and social engineering attacks. Again, what matters is forward progress and continuous improvement, more than an end state of perfection. Most of the best security training platforms will provide summary and detailed reporting showing progressive improvement by individuals, teams, departments, and the company as a whole. Leaders will want to study training adoption, quiz and test results, and the progressive improvement in regular testing exercises, like the phishing tests mentioned above.

> *It cannot be repeated enough, people are the weakest link in cyber security.*

Assume Breach

5

We live and work in a fluid and fast changing environment. Companies are becoming more distributed. Employees are working in the office, on the road, in home offices, and on the go from mobile devices. Corporate data lives more places, including on laptops, mobile devices, and in the cloud and on SaaS services. Sensitive corporate data, intellectual property, and trade secrets are no longer safely guarded behind the corporate firewall.

Therefore, it makes sense assume that a security breach of some sort of is inevitable. It is a case of when, not if.

Naturally, any and all measures should be employed to prevent a breach from happening in the first place. But with the current threat environment, complexity of IT systems, and inevitable employee mistakes, it is best to assume that a breach will occur.

But what then is the solution?

The first part of the solution is to implement a principle of least privilege, which specifies that employees must be able to access only the information and resources that are strictly necessary to do their job well. Too often, haste and sloppiness leads to employees being granted access to systems and data that are unnecessary to the performance of their jobs. When things are too loosely implemented, even good employees sometimes fall prey to snooping or theft of data which is extraneous to their job function. The problem is only compounded with malicious or disgruntled staff. In other scenarios, an overly privileged user may be compromised by a bad actor, giving them access to sensitive systems and data.

The second part of solution is to invest in data leak prevention (DLP) technology. DLP technology prevents the exfiltration of data en masse. Various forms of data can be tagged with different levels of sensitivity. And in turn, steps are automatically taken to prevent certain kinds of data from being copied/pasted, uploaded, or saved, into an email, folder, or other cloud system. Additional measures can work in concert with DLP, such as outbound email filtering and mobile device management (MDM). Outbound email filtering can detect and/or prevent employees from emailing themselves or others sensitive company information, such as client lists, data containing health records or social security numbers, or intellectual property. MDM also provides many of these same functions on mobile devices, which are easily lost or stolen. In a mobile setting, the ability to remotely wipe corporate data off of a device is a key remedy in many scenarios. Lastly, many cloud and SaaS applications have rich sets of controls which allow for least privilege implementations and measures to prevent the mass export or exfiltration of data.

At the end of day, whether it is employees or bad actors who have gained unauthorized access, it is best to assume breach and protect a company's data appropriately.

It makes sense assume that a security breach of some sort of is inevitable. It is a case of when, not if.

Clearly Define Responsibilities

6

The next step is to clearly define responsibilities. Many small businesses contract with an IT service provider to deliver outsourced IT management. Unfortunately, in many of these engagements, there is no detailed scope of work in place. The firm simply gets hired and onboarded with a poorly documented scope of work and a fuzzy set of responsibilities. Alas, many firms get hired in a crisis and the emphasis is often “simply make my IT headaches go away.” This is a pretty scary situation, as the IT service provider is often highly privileged in nearly all systems, with sensitive access to everything in the company.

For internal staff, the same principles apply. First, as discussed above, the principle of least privilege should be implemented. There needs to be clarity on the various functional areas of responsibility and who does what. itSynergy recommends an internal Accountability Chart. This is not unlike an org chart, but in this case we are mapping functional responsibilities to different staff members and clearly documenting all the details.

As your organizational evolves and changes, it is vital to keep the Accountability Chart up to date. Employee turnover is a huge challenge. The problem is compounded when internal changes to access and accountability are not thoroughly documented and tracked. Like with risk management, this is an ongoing process since people are always coming and going in an organization.

The OCIE inspectors are looking for thoroughly documented accountability and follow through and discipline in the implementation.

Risk Management Doesn't Mean Risk Mitigation

7

A culture of risk management is the last element in building your cyber security and compliance foundation. Discussing risk management can often be scary and overwhelming for some. As we have seen throughout this whitepaper, there are manifold risks to the privacy, security, and operations of your firm. There are external threats, internal bad actors, and employee negligence that can all lead to breaches and financial losses.

The goal for leadership is to break down and prioritize these risks and methodically manage them in the right order. Perfection is the enemy of the good and paralysis is not an option. The reality is however, no organization has unlimited resources to mitigate 100% of every risk in a short amount of time. On the contrary, resources of time, money, and staff are often scarce and it is vital to properly prioritize the risks that can cause the greatest damage and to tackle them in the right order. This reality is not lost on regulators and inspectors. The expectations for a ten person firm will be vastly different than for those of a 100 or 1,000 person firm. Ultimately, the test is reasonableness, based on a firm's size and resources.

A culture of risk management embraces the transparent analysis of risks and puts in place a proactive process to manage the risks. For RIA firms to maintain compliance, it is vital that all the foundational elements discussed in this whitepaper are implemented and a culture of risk management and compliance is cultivated.

A culture of risk management embraces the transparent analysis of risks and puts in place a proactive process to manage the risks.

Conclusion and Getting Started

At itSynergy, we specialize in helping RIAs develop a culture of risk management and compliance, through prudent investments in cyber security. We invite interested firms to get to know us by inviting us to conduct a risk assessment for your firm. As we have shown throughout this whitepaper, itSynergy's rigorous approach will help you identify and manage your risks and start down the path of building a solid a cyber security and compliance foundation.

About itSynergy

itSynergy specializes in helping registered investment advisers grow profitable businesses. itSynergy helps our clients tame their information technology, so they can securely and efficiently focus on their core business. Serving clients throughout the Phoenix and Denver metro areas, itSynergy delivers compliance, cyber security, and managed IT services to investment advisory firms. The company is led by president and founder Michael Cocanower. Mr. Cocanower has over 25 years of experience in the IT field. Mr. Cocanower has been recognized as a Microsoft® Certified Professional and Microsoft® Most Valuable Professional as well as a Certified Ethical Hacker.

Copyright © 2020 MC Group, Inc. All Rights Reserved.
All third party trademarks belong to their respective owners.

www.itsynergy.com
(602) 297–2400

PEOPLE INNOVATION RESULTS
itSynergy®