charles SCHWAB

Compliance Review

Ongoing compliance updates for independent investment advisors

July 2020

Advisor Services

IN THIS ISSUE

Practical cybersecurity for advisors: Keeping up with the evolution of best practices

E.J. Yerzak, CISA, CISM, CRISC, Director of Cybersecurity Services, Compliance Solutions Strategies

I. Introduction

It's Monday morning. You've barely had time to set your coffee down on your desk and pull up your email when a panic-stricken coworker steps into your office unannounced. Your colleague can barely get his words out, but somehow you know what's coming: "I think we've had a data breach." As the reality sets in, you find yourself at a loss for words. The two of you ask each other, in unison: "What do we do?"

If this scenario sounds familiar, welcome to the club. Perhaps you can count yourself among the lucky ones who at least knew something was compromised. As the oft-quoted line goes, "There are two types of companies: those who know they've been hacked and those who don't know they've been hacked." And while movies tend to portray hacking as a drama-filled race featuring hooded figures spouting technology buzzwords as they try to bypass firewall security, cybersecurity attacks are not always complex. In reality, your firm is more likely to suffer a data breach at the hands of its own staff. Unfortunately, humans are the weakest link in any company's security. Unpatched systems enable even moderately skilled hackers to exploit the same vulnerabilities over and over. When a firm gives full administrator rights on computers to everyone at the firm, these exploits become even more dangerous.

Complex attacks do still exist, however. Cyberattacks have increased in both volume and sophistication over the years. Advanced persistent threats, in which nation state–sponsored attackers specifically and methodically target firms and remain in their systems for months without being discovered,[1] have led the Department of Homeland Security to label cyberattacks a larger threat to U.S. critical infrastructure than terrorism. As more firms operate in the cloud through email, file sharing, and trading through their custodian, and as detection capabilities improve, hackers work to evolve their techniques and methods.[2] Malware can now be purchased online as easily as adding an item to your cart on Amazon (malware marketplaces have shopping carts, too).

Financial services has been designated as a sector of critical infrastructure in the U.S. It is therefore not surprising that financial services firms are a major target[3] and that the cost of data breaches continues to rise. Phishing attacks seeking to gain user credentials are a growing problem for financial services firms, particularly due to the sensitivity of the data that can be accessed with such credentials.

[1] Industry surveys note that 41% of incidents (typically ransomware) are detected in 30 days or fewer, while 59% of incidents take longer to detect and 12% take over 700 days to detect. See "FireEye / Mandiant M-Trends 2020 Special Report."

[2] Common anti-virus and anti-malware solutions look for patterns or digital fingerprints of known malware. By changing a small part of the malware, hackers can create a new variant that evades detection because it no longer matches any known patterns. FireEye reports that 41 percent of the malware it observed was new in the past year. See "FireEye / Mandiant M-Trends 2020 Special Report."

[3] Approximately 10 percent of all data breaches occur in the financial industry. See "2019 Data Breach Investigations Report," Verizon.

"We think of email as cyber public enemy number one."

Adam Moseley
Director, Technology Consulting
Business Consulting and Education
Schwab Advisor Services

While employee negligence or recklessness contributes to many breaches, particularly with respect to falling for phishing attacks, targeted attacks of senior executives by sophisticated hackers are also an ongoing concern. The expansion of U.S. and international data privacy regulations, such as the California Consumer Privacy Act (CCPA) and the EU's General Data Protection Regulation (GDPR), have increased the cost of both compliance and incident response (IR). IR costs include forensic analysis of the breach, legal consultation, disclosure, and (perhaps most significantly) the financial impact of reputational harm and its attendant client churn. These data privacy regulations also highlight the need for robust data classification processes that allow firms to identify all the places where a particular individual's data may be stored.

Investment advisors are urged to pay close attention: The Securities and Exchange Commission (SEC) observed years ago the "mounting evidence that the constant threat of a cyber-attack is real, lasting, and cannot be ignored."[4] Yet the threat has proven to be even more challenging than regulators may have anticipated, given the ease with which hackers have launched armies of compromised machines and devices to bring down entire swaths of the Internet, as well as the breadth of compromised personal information for sale on the dark web. Regulatory awareness of the threat is evident in the number of cybersecurity risk alerts which continue to be issued by the SEC, the Financial Industry Regulatory Authority (FINRA), and state regulators—including on topics such as ransomware.[5]

Discussions of cyberattacks are no longer confined to security researchers; they are front-page news, with data breaches involving major retailers and service providers regularly making national headlines. For example, the world has witnessed firsthand how:

- Deep-fake videos and social media bots can be used to target and manipulate people with stunning precision regarding election messaging.
- Cyberattacks against the expanding universe of Internet of Things (IoT) devices, such as unprotected home video cameras and home voice assistants, can easily be used to launch denial of service attacks to bring any website or online service to a halt, as Netflix experienced firsthand when it was brought offline after being targeted by an army of compromised "smart" devices.[6]

It is only a matter of time before these same techniques are used against advisory firms in a similar fashion. Consider, for example, a deep-fake video that purports to show a firm's investment team touting a specific security to buy, enabling the hacker to generate demand among the advisor's clients and front-run the trades for a profit. Related to this last point, regulators have taken notice that hackers are also targeting financial firms for their trading ideas and sensitive emails, seeking to profit through insider trading as well as extortion.

What has changed significantly over the past several years with respect to cyberattacks is public consciousness. Security professionals and nonprofessionals alike are increasingly aware that cyberattacks and data breaches are a question of "when," not "if," and that this apparent inevitability has become part of the cost of doing business. And in an interconnected world, a cybersecurity incident occurring at an advisor's service provider, such as a custodian or fund administrator, could have significant downstream implications for the advisor itself if not managed effectively.

II. Regulating cybersecurity

Regulators are also paying more attention to cyberattacks and are increasingly taking a coordinated approach to risks, suggesting that advisors may find helpful tips not only in SEC guidance but also in best practice tips released by other regulatory bodies, including FINRA and the Commodity Futures Trading Commission (CFTC). Such a coordinated approach may prove helpful even to firms not registered with these other bodies.

The SEC and cybersecurity

The SEC, recognizing the growing need for strong cybersecurity controls at investment advisory firms faced with increasing incidents of hacking and wire fraud, has included the topic of cybersecurity as one of its examination priorities nearly every year over the past decade.

Regulation S-P, in place since June 29, 2000, forms the basis for advisors to adopt policies and procedures that are "reasonably designed to: (i) ensure the security and confidentiality of customer records and information; (ii)

[4] Luis Aguilar, "The Commission's Role in Addressing the Growing Cyber-Threat," SEC Cybersecurity Roundtable (March 26, 2014).

[5] OCIE Risk Alert, "Cybersecurity: Ransomware Alert" (May 17, 2017).

[6] In November 2016, the Mirai botnet cyberattack involved over 600,000 IoT devices that had been previously compromised. The devices were simultaneously directed by a command and control (C&C) server to attack the same targets, including the Domain Name Server (DNS) that is used to help the public find and access many popular websites. With the DNS server unavailable, websites and services such as Amazon, Netflix, and Twitter experienced disruptive unavailability, even though they were not the direct target. This botnet attack highlights how an attack on one service provider can have collateral damage to downstream third parties.

protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (iii) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."

Regulation S-ID, a joint rule by the SEC and CFTC and effective since 2013, requires that certain financial institutions adopt and implement an identity theft prevention program. Regulation S-ID is largely intended to address the risk of fraudulent wire transfers by mandating controls to identify, detect, and respond to red flags of identity theft. Examples of such red flags include the presentation of suspicious personal identifying information (such as a driver's license that appears to be forged or personal details that do not match information that the advisor knows or can reasonably verify), wire requests that differ in frequency and amounts from historical activity on a given account, and communication from a client stating that they believe their email account has been hacked. The increased frequency of phishing emails has certainly contributed to a higher risk of identity theft for many firms.

In addition, the SEC has proceeded through several phases of its Cybersecurity Examination Initiative, during which time the agency has conducted cybersecurity sweep examinations of registered investment advisors to assess their cybersecurity posture. The SEC's cybersecurity focus comprises seven broad topics:

- Governance and risk management
- Access rights and controls
- Data loss prevention
- Mobile security
- Incident response and resiliency
- Vendor management
- Training and awareness

In practical terms, the SEC is essentially seeking answers to some basic cybersecurity questions, which can be summarized as follows:

Does the firm know what information it is trying to protect and where that information is?

The SEC may request that firms provide inventories of hardware and software, network maps, data flows, data classification, and details of how such information is logged. For firms that have undergone mergers and acquisitions or that have multiple offices, the SEC may ask about the status of integration of firm systems, as well as the integrity and security of data when the same data is stored in multiple, disparate locations across firms.

How does the firm protect the information it deems sensitive?

In other words, has the firm adopted a written information security program (WISP) with clearly defined cybersecurity roles and responsibilities, network access provisioning controls, encryption, patch management processes, and segregated development, test, and production environments for proprietary development?

How does the firm monitor and detect access to information?

The SEC may ask whether the firm conducts periodic vulnerability assessments (including vulnerability scanning, penetration testing, and phishing testing), whether security awareness training is conducted for staff, whether data loss prevention (DLP) controls are in place, how the firm monitors baseline configurations of networks and systems against events, how unauthorized users and devices are detected, and how the firm exercises oversight with respect to third-party service providers, including revoking access from terminated staff and vendors in a timely manner.

How does the firm respond to data breaches?

The SEC may delve into the firm's incident response plan, including the investigation and reporting process, whether any incidents have occurred and the nature of such incidents, and whether claims were made against any applicable cybersecurity insurance policies.

Fortunately for advisors, SEC staff have also issued several risk alerts on cybersecurity, putting firms on notice of certain practices that it considers to be concerning or notable. The risk alerts include the following topics:

- Ransomware[7]
- Electronic Messaging[8]
- Regulation S-P Privacy Notices and Safeguard Policies[9]
- Safeguarding Customer Records and Information in Network Storage / Use of Third Party Security Features[10]

Cybersecurity and resiliency

To learn more about the SEC's cybersecurity focus areas, read the Cybersecurity and Resiliency Observations report from the Office of Compliance Inspections and Examinations.

[7] OCIE Risk Alert, "Cybersecurity: Ransomware Alert" (May 17, 2017).

[8] OCIE Risk Alert, "Observations from Investment Adviser Examinations Relating to Electronic Messaging" (December 2018).

[9] OCIE Risk Alert, "Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies" (April 16, 2019).

[10] OCIE Risk Alert, "Safeguarding Customer Records and Information in Network Storage – Use of Third Party Security Features" (May 23, 2019).

Both the SEC's and FINRA's focus on cybersecurity have provided some much-needed guidance to the industry. We now know what the examiners are looking for, and what they are expecting, with respect to cybersecurity controls at firms. While the initial sweep exams were originally touted as a benign investigative effort to benchmark industry best practices, firms are now on notice of regulatory expectations in this area. Inadequate measures to address cybersecurity are ripe for citation in deficiency letters.

The SEC, recognizing the growing need for strong cybersecurity controls at investment advisory firms faced with increasing incidents of hacking and wire fraud, has included the topic of cybersecurity as one of its examination priorities nearly every year over the past decade.

The SEC has also been willing to bring enforcement actions against investment advisors in certain instances, and it has established a Cyber Enforcement Actions spotlight page on its website where the public can track such cases.[11] Among the notable cases are several related to hacking by employees and by external parties for insider trading purposes, a case involving inadequate cybersecurity policies designed to mitigate customer account compromises after phishing attacks,[12] a case involving firm data transferred by an employee to a personal server that was subsequently hacked,[13] and numerous actions brought against companies other than advisory firms for failures to disclose cybersecurity breaches and for fraudulent initial coin offering (ICO) and cryptocurrency-related activities.

The various enforcement actions brought against advisors share a common theme: The SEC expects firms to have cybersecurity policies and procedures that are accurate and consistent with actual practices, tailored to their specific controls and systems, and followed by employees, and it expects cybersecurity risks identified through regular risk assessments to be prioritized and remediated, rather than ignored.

FINRA's focus on cybersecurity

FINRA reviews privacy controls at member firms, and its examinations include detailed reviews of cybersecurity controls. FINRA's annual Risk Monitoring and Examinations Priority Letter includes a focus on electronic communications channels, change management controls for technology changes relating to market access systems, and cybersecurity issues relating to firm operations.

FINRA has at times conducted cybersecurity sweep examinations of various member firms to assess the cybersecurity threats facing these firms and to understand the firms' risk assessment processes, controls, and practices to manage and mitigate those threats.

FINRA has followed up its examinations by publishing its Report on Cybersecurity Practices, in which it notes several effective practices, including the use of written supervisory procedures to establish minimum cybersecurity standards for branch offices; the aggregation of inventories of data, hardware, and software across branches to identify what data is stored where; the use of standard hardware and software configurations across branches; and security awareness training and alerts communicated to branch employees. FINRA also highlights the effectiveness of practices including regular permission reviews, data loss prevention controls, phishing testing and training, and security information and event management (SIEM) network monitoring tools.

CFTC guidance

All financial institutions, especially those engaging in swaps and derivatives trading and which are therefore subject to CFTC oversight, are well advised to heed guidance from the CFTC. The CFTC regulates cybersecurity through its system safeguards rules (17 C.F.R. §§ 1,3, and 23), which require designated entities under the CFTC's jurisdiction to implement cybersecurity programs. Whereas SEC guidance tends to be principles-based, the CFTC specifically mandates the testing and monitoring of system safeguards. CFTC rules define five categories of required cybersecurity testing as shown below, with a frequency determined reasonable based upon a firm's risk assessment. Certain firms that are deemed Enhanced Covered Entities have stricter testing frequencies (shown in parentheses):

- Vulnerability testing (at least quarterly)
- Penetration testing (at least annually)
- Controls testing (a rolling basis is recommended, but at least every three years)
- Security incident response plan testing (at least annually)
- Enterprise technology risk assessment (at least annually)

[11] See SEC Cyber Enforcement Actions.

[12] In re: Voya Financial Advisors, Inc., Admin. Proc. File No. 3-18840.

[13] In re: Morgan Stanley Smith Barney LLC, Admin. Proc. File No. 3-17280. (A separate action was brought against the employee.)

While the CFTC testing requirements and frequencies are intended for CFTC Covered Entities, they are also advisable for registered investment advisors of all sizes. Since the cost of retaining a third-party vendor to conduct such testing is typically based upon network size and similar variables, small advisors will likely find that they can accomplish meaningful cybersecurity testing at a reasonable cost relative to their size and budget.

Data protection at the state level

In addition to the guidance on cybersecurity that has been issued by federal regulatory bodies, the state legislatures have been very active in enhancing data protections for residents of their respective states. All 50 states have a data breach notification law in effect now, which was not the case when the SEC first began its cybersecurity examinations. Furthermore, several states appear to be following the GDPR data privacy model in designing their own state privacy requirements. Massachusetts, one of the first states to mandate specific data protections for its residents, is now joined by states such as New York (with its New York Department of Financial Services Cybersecurity Regulation, as well as its SHIELD Act) and California (with its CCPA). The CCPA largely mirrors the privacy rights conferred on EU residents under the GDPR and includes provisions such as requiring covered firms to respond to consumer requests to provide the data they have collected regarding the consumer and to delete such data upon request, unless an exception applies. It appears that other states are moving in a similar direction in terms of adopting stronger data privacy requirements, resulting in a patchwork of standards for organizations with clients in multiple states.

Certain states do include exceptions to their data privacy laws with respect to data that is already subject to protections under the Gramm-Leach-Bliley Act (GLBA), whereas other states extend the exception all the way to any firms governed by the GLBA. And regardless of the applicability of any exemptions, advisory firms that are federally registered with the SEC are still obligated to maintain required books and records under Advisers Act Rule 204-2.

State-registered advisors may find helpful guidance from the North American Securities Administrators Association (NASAA), which represents state securities regulators. In 2019, NASAA membership adopted a model rule for state regulators to consider adopting: the "Investment Adviser Information Security and Privacy Rule."[14]

III. Understanding the NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework, while highly technical, is nonetheless accessible and understandable. In fact, the framework is intended to be technology-agnostic and sector-neutral, meaning that its guidance can be used regardless of the type of industry, size of firm, or technical background of personnel.

Rather than mandate cybersecurity legislatively, which would be quite difficult to enforce as a universal standard across industries with unique risks and characteristics, the framework is a "voluntary" one. It approaches cybersecurity as a collective bar that can be raised through the collaboration of the public and private sectors in developing best practices and sharing information on cybersecurity threats. Notwithstanding the voluntary nature of the framework, investment advisors are reminded that the SEC's cybersecurity sweep was largely modeled after the framework.

How can the NIST Cybersecurity Framework help?

The framework enables advisors to benchmark cybersecurity at their firms through a standardized set of controls and practices. The framework consists of:

- ✓ A framework core
- ✓ Framework implementation tiers
- ✓ Framework profiles

The framework was first released in 2014 and has been updated since then to enhance details relating to identity management and supply chain risk.

Looking for more information on compliance or regulatory issues?

The Schwab Advisor Center compliance page includes additional Compliance Review papers to assist you.

[14] "Investment Adviser Information Security and Privacy Rule" (adopted May 19, 2019).

Framework core

This part of the framework includes five cybersecurity functions: identify, protect, detect, respond, and recover (see Figure 1). Within each function are categories and subcategories of information security practices related to that function. For example, the "identify" function (ID) includes categories such as asset management (ID.AM) and governance (ID.GV).

The asset management category includes subcategories such as ID.AM-1, which asks whether the firm has established an inventory of all physical devices and systems within the organization; ID.AM-2, which asks whether the firm maintains an inventory of all software and applications; and ID.AM-3, which asks whether the firm has created a map of data flow between systems.

Each subcategory is listed along with accompanying references to established standards, guidelines, and practices, including COBIT 5, NIST, and ISO/IEC 27001:2013.

Framework implementation tiers

Implementation tiers provide a way to map a firm's continuous state of improvement as well as current and target risk tolerances. According to NIST, although the framework is not a maturity model, firms are urged to strive toward building up their information security programs to higher implementation tiers according to described criteria. There are four implementation tiers, ranging from ad hoc, reactive practices to established, planned practices. Taking into account factors such as a firm's risk management process, the involvement of senior management, employees' awareness of their cybersecurity roles and responsibilities, and the ability to collaborate and communicate with third parties with respect to cybersecurity, firms can be categorized as having an information security program in one of the following tiers:

1. Partial
2. Risk-informed
3. Repeatable
4. Adaptive

Framework profile

Within each subcategory in the framework, firms can document their existing current profile and their planned target profile. For example, an advisor may state that with respect to PR.DS-1, it currently does not protect data-in-transit and generally sends client statements via email, but that it is in the process of implementing a secure client/investor portal that will use encryption for data-in-transit.

Figure 1:
The NIST Cybersecurity Framework core

Function unique identifier	Function	Category unique identifier	Category
ID	Identify	ID.AM	Asset management
		ID.BE	Business environment
		ID.GV	Governance
		ID.RA	Risk assessment
		ID.RM	Risk management strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management, authentication and Access control
		PR.AT	Awareness and training
		PR.DS	Data security
		PR.IP	Information protection processes and procedures
		PR.MA	Maintenance
		PR.PT	Protective technology
DE	Detect	DE.AE	Anomalies and events
		DE.CM	Security continuous monitoring
		DE.DP	Detection processes
RS	Respond	RS.RP	Response planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery planning
		RC.IM	Improvements
		RC.CO	Communications

Source: National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity"

Regulators are using the NIST Cybersecurity Framework

NASAA's model cybersecurity rule is informed by the NIST Cybersecurity Framework. In fact, NASAA's model rule includes a requirement for advisors to establish, implement, update, and enforce written information security policies and procedures that cover the five functions listed in the framework. NASAA has also provided a free cybersecurity checklist[15] as a resource for state-registered advisors to evaluate their cybersecurity programs; however, small and medium SEC-registered advisors may find the resource helpful as well.

Many of the cybersecurity risk topical areas identified by FINRA, the SEC, the CFTC, and state regulators are addressed in the NIST Cybersecurity Framework.[16] The financial industry can benefit from the framework's guidance, which is specifically referenced in the SEC's cybersecurity examination initiatives by way of footnote. The development of this standard was mandated by Executive Order 13636 ("Improving Critical Infrastructure Cybersecurity"). Advisory firms are therefore well advised to be familiar with this framework when evaluating how their cybersecurity programs stack up against their peers, and whether the programs are addressing the right risks.

Best practices identified by regulators

Notable practices identified by the SEC through its various risk alerts include:

- Restricting which electronic messaging and social media platforms and apps can be used for business purposes.
- Developing detailed cybersecurity policies and procedures that not only go well beyond the Reg. S-P and Reg. S-AM notices about what data is collected and shared, but also do more than simply confirm that the required administrative, technical, and procedural controls are in place to safeguard the data. The cybersecurity policies should detail what those controls entail, such as hardware and software inventories, physical security, access provisioning and deprovisioning, use of encryption, password controls, mobile devices, patch management, and other areas.
- Making security awareness training mandatory for all staff, maintaining evidence of completion, and imposing penalties for non-compliance.
- Taking advantage of enhanced security controls, such as multi-factor authentication (MFA), when offered by cloud-based service providers.
- Conducting ongoing due-diligence reviews of vendors.
- Classifying data based on sensitivity, inventorying what data is stored where (internally and with which vendors), and identifying which vendors have access to a firm's network.
- Implementing system hardening practices, including changing default passwords.

Among the best practices recommended by the CFTC in Staff Advisory 14-21:

- Designate an employee, reporting directly to senior management or the board of directors, specifically tasked with oversight of privacy and information security.
- Perform risk assessment and business impact analysis to establish an understanding of current security risks and to assess the security impacts of any changes to systems.
- Create a written information security program (WISP).
- Train employees periodically with respect to cybersecurity.
- Regularly test the effectiveness of cybersecurity controls, including encryption and the ability to detect and respond to incidents involving unauthorized access.
- Retain an independent third party to perform an information technology risk assessment.
- Implement an incident response plan.

These best practices are derived from both SEC risk alerts and the CFTC. While the SEC has provided best practices in risk alerts, the CFTC has actual regulatory requirements as found in its Staff Advisory 14-21 that you should keep in mind if you're subject to CFTC oversight.

[15] North American Securities Administrators Association, "Cybersecurity Checklist for Investment Advisers" (issued in 2017).

[16] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity" (April 2018).

IV. Getting practical about cybersecurity: What can we do?

Against the twin backdrop of the increase in cyberattacks and heightened regulatory scrutiny, what are investment advisors supposed to do—go back to a completely paper-based system and completely disconnect from the Internet? Since that is not practical, it raises the questions: How can we achieve cybersecurity without spending a fortune? Is there such a thing as "enough security"? How can we get the most bang for our buck and implement cost-effective controls that are, in the words of Advisers Act Rule 206(4)-7, "reasonably designed" in light of our firm's anticipated risks, size, business model, resources, budget, and risk tolerance?

In addition to following the specific best practices delineated by the SEC and CFTC in the callout box on page 7, you should also consider whether the following cybersecurity controls may be appropriate for your firm:

- File- and folder-level access controls employing the concept of least privilege, so that no employee has access to any files beyond that employee's job function.
- Regular reviews of access controls to audit permissions and to ensure that access for terminated staff and vendors is revoked promptly.
- Mobile device management (MDM) controls, such as using Microsoft Exchange ActiveSync or a third-party vendor to perform a "remote wipe" of lost or stolen mobile devices. This technical solution should ideally be combined with training to properly safeguard such devices in the first place and a clearly defined reporting process.
- Implementation of multi-factor authentication for cloud-based systems whenever feasible. Since many people still tend to reuse the same usernames and passwords across multiple websites, the compromise of those credentials on one site could enable a hacker to access any other site where the same credentials are used. A second factor of authentication, such as a one-time password or PIN generated on a token or through an authenticator app, can help keep accounts secure.
- Encryption for data-in-transit. Where feasible, enable support for TLS 1.2 or 1.3 and disable support for older or weaker encryption, including TLS 1.0, TLS 1.1., and SSL.

Visit Schwab's Cybersecurity Resource Center

Schwab Advisor Services has resources available to help you strengthen your cybersecurity program, including educational materials, actionable tools, and third-party resources. Visit schwabadvisorcenter.com to access these resources.

- Encryption for data-at-rest, such as the use of 256-bit AES encryption. Bitlocker encryption offers encryption at rest for Windows PCs, but it is important to confirm that the encryption is actually turned on.
- Data loss prevention (DLP) tools. For example, this technology can alert compliance and IT personnel when an individual is attempting to email sensitive data outside the firm. Some DLP software can automatically encrypt the message before sending or can be configured to block the message entirely (for example, an email to an entire client list sent offsite by an employee who is planning to leave the firm).
- Network monitoring tools, including intrusion prevention systems (IPS) and intrusion detection systems (IDS), and a routine review of access logs.
- Storage of firewall and other access logs, when feasible, in a separate location other than on the firewall itself. This can both increase the number of logs that can be stored before they are overwritten and prevent the logs from being altered by a hacker seeking to cover his or her tracks.
- Restrictions on the use of USB/flash drives or other portable media that may be insecure or contain malware.
- Continuous assessment. Cybersecurity threats and risks are constantly evolving, and your risk controls should do the same. Consider third-party cybersecurity risk assessments and technical testing (vulnerability scanning, penetration testing, and phishing testing) to supplement your efforts to stay ahead of the cybercriminals. For firms with an IT vendor in place, ideally you wouldn't want them to test their own controls, as this would be akin to the fox guarding the hen-house. A third-party cybersecurity audit can serve as a spot check on the effectiveness of your controls.
- Conducting security awareness training for all new hires, and requiring all staff to complete annual security training thereafter. Regulators expect to see evidence that training was not just offered to staff, but was actually conducted and completed. Cybersecurity is everyone's responsibility, not just that of the IT team. Since everyone at your firm is in a position to either prevent or cause a cybersecurity incident, training for all staff is a crucial component of a strong cybersecurity program.
- Annual (or more frequent) review of cybersecurity policies and procedures to confirm that they remain accurate in light of any changes your firm may have made to its systems, applications, staff, and operational processes. References in policies to outdated systems or staff who are no longer with the firm can suggest to regulators a stale cybersecurity program without adequate oversight.

- Implementation and testing of an incident response plan through tabletop exercises and simulations. Security incidents can occur at firms of any size and shape. It is important to have a list of steps to follow when responding to an incident, because time is critical and malware may continue to cause harm on your network if you don't act quickly. If ransomware strikes, should you unplug the machine right away or notify IT staff first? Should an advisory representative who caused a data breach reach out to an affected client immediately, or wait for an official message to be crafted by the marketing department? Incident response plans can be tested by walking through various likely scenarios with your staff to ensure they know who is responsible for doing what, how and when impacted clients will be contacted, and which third-party providers the firm may need to rely upon for assistance with forensic investigation of logs and breach notification.

Finally, a cost-benefit analysis should be a critical component of any risk management process. In a world where advisors are constantly playing catch-up with the evolving techniques of cybercriminals, security can never be 100%. But with the right mix of sound policies and procedures, coupled with the right technology and effective testing, advisors should be able to rest easily at night knowing they've done all they can to protect their firms.

Cybersecurity threats and risks are constantly evolving, and your risk controls should do the same. Consider third-party cybersecurity risk assessments and technical testing (vulnerability scanning, penetration testing, and phishing testing) to supplement your efforts to stay ahead of the cybercriminals.

V. Incident management and response

The NIST Cybersecurity Framework, via the Respond and Recover Function, and the SEC's examination priority focus on incident response and resiliency have placed a clear spotlight on incident management and response capabilities. But what do these mean in practice? And how can smaller advisors become confident that they can handle a security incident?

Consider the following practical guidance:

1. Identify events or potential incidents through a "vulnerability management" process that likely includes various methods of aggregating information, such as monitoring your firewall. If your firm has intrusion detection/prevention capabilities, take the time to do the following:

   - Set up alerts for unauthorized devices or connections.
   - Track patterns of anomalous activity when compared to your baseline. For example, if employees do not typically come in on the weekends or work from home, then a significant spike in network traffic during these hours may indicate that files are being accessed or a large data transfer offsite is occurring.
   - Scan servers, workstations, and devices for malware and potential exploits.
   - Examine system logs for unauthorized activity or movements throughout your network, even by internal staff.
   - Maintain open communication with well-trained workers who will escalate concerns to appropriate or designated personnel in a timely manner.

   Many small firms do not have the budgets for significant logging capabilities, and often store as little as 30 days of firewall logs on the firewall itself. Since the average time a hacker is on a firm's network before being detected (and the incident contained) is approximately 279 days, the importance of adequate logs to support your investigation cannot be stressed enough.[17] Without sufficient logs, you may not be able to rule out that a security incident was a reportable data breach. With such logs, you may have proof that a hacker accessed only a certain file or folder and did not proceed further. While smaller firms might not be able to afford a Security Incident and Event Management (SIEM) application, they should at least consider copying log files to separate read-only storage to avoid having only one copy of log files that may be overwritten.

2. Investigate incidents thoroughly, and document all actions taken when conducting forensics, isolating systems, or identifying potential threats. For a consistent and effective response to identified events, address the categorization of severity and methods for prioritizing events, including defining specific personnel and teams (such as an incident response team) for conducting analysis, determining impact, and formulating an appropriate response. For example, a phishing email that was identified and reported may have a lower risk category than a ransomware event that is currently in progress locking all of a firm's files.

[17] The Ponemon Institute 2019 Cost of a Data Breach Report notes that the average data breach life cycle is 279 days, representing an increase of 4.9% from the prior year.

3. Mitigate incidents according to categorization. For example, malware identified on a workstation through scanning may require isolation, additional scanning, and validation of eradication of infected files. A potential email phishing scam may require immediate action from response personnel to alert employees and ensure that risks related to any exposure of credentials is addressed immediately (e.g., by conducting an immediate password reset and placing the account under heightened monitoring for anything suspicious). The loss of a cellphone or device that accesses corporate email may require a "remote wipe" and the issuance of new access credentials. Naturally, the most damaging forms of breach could involve the loss of client information, in which case detailed forensics, legal research on state breach requirements, potential notification to clients, and management of any resultant public relations issues may be necessary.

   Specific steps for mitigation should be planned in advance and well understood. Advisors must also consider whether identified and mitigated incidents represent potential attempts at identity theft, which would require the documentation of such events as red flags according to Regulation S-ID.

4. Post-incident assessment in its simplest form involves reviewing incidents and actions taken, making sure you have acted in line with existing policies and procedures, including documenting and determining lessons learned for improvement of your plan and identification of potential training opportunities. In one case, the SEC brought an enforcement action against a firm that observed evidence of phishing and failed to act promptly to prevent further account compromise.

   Prioritization of actionable items, as well as records of process ownership and accountability for implementing enhancements to your procedures and systems, can serve as evidence to examiners that you have developed plans for improvement. While some firms may be reluctant to document their incidents in vivid detail, a reasonable, cost-effective strategy for remediation may paint the picture of a strong culture of compliance and cybersecurity at your firm.

5. Finally, take the time before a security incident occurs to conduct reasonable due diligence on your third-party service providers, including your custodians. Understand how a security incident at your firm may impact downstream entities, as well as how an incident at one of your providers can impact operations at your firm. What are the service provider's or vendor's notification procedures to alert you to an incident? What timeframe do they guarantee for such notification? NIST includes specific references to the importance of managing vendor risk.

   Many security experts and advanced IT personnel concur that security incidents and breach are inevitable. Failing to plan for managing incidents and events is unacceptable. That is why we see such a strong regulatory focus on policy and procedure creation, training, and awareness.

Other cybersecurity resources and information

- ✓ The NIST Information Technology Portal contains a wealth of information, white papers, and protocols for addressing the assessment of specific IT issues.
- ✓ The Cloud Security Alliance serves up best practices for use and security of cloud-based technology and principles applicable to all IT programs.
- ✓ The US-CERT (Computer Emergency Readiness Team) provides timely information on threats, vulnerabilities, and specific exploits. Sign up to receive alerts to satisfy the concept of assessing threats and vulnerabilities on a continuous basis.
- ✓ The FS-ISAC (Financial Services–Information Sharing and Analysis Center) is both a source for information about threats specific to the financial sector and an avenue to share information concerning incidents identified at your firm. The concepts of sharing and good corporate citizenship are part of the NIST Cybersecurity Framework Implementation Tiers and demonstrate your firm's understanding that you are part of a larger security ecosystem.

VI. Conclusion and key takeaways

Cybersecurity is a vast topic that requires a healthy collaboration between compliance and IT. The intersection of this collaboration starts with an appreciation that cybersecurity risk is a firm-wide risk, and not just a risk relegated to the IT staff. Regulators have an expectation that cybersecurity is considered in your risk process. We are beyond the concept of risk management; regulators expect that you will have a regular risk assessment process that incorporates cybersecurity and that action items for remediation are prioritized and implemented. These practices, from both a regulatory and implementation standpoint, boil down to healthy communication at your firm. For larger firms, cybersecurity is a board-level issue due to the nature of business risk and the resulting expense related to breach. Breach of information is often referred to as the "seven-figure problem" because of the resources needed to thoroughly address forensic, legal, and reputational issues. While smaller advisors may not have a board, regulators would nonetheless expect that cybersecurity risks at such firms be thoroughly understood at the executive management level.

At an Ascendant compliance conference, the chief compliance officer from a major fund complex once mentioned that he "has had to become an IT person in order to keep up with the changing landscape." For chief compliance officers and others in operational risk roles, there are several resources available to assist in understanding basic controls and information practices that are, in some cases, foundational to the NIST Cybersecurity Framework. Such an understanding leads to a growing sense of confidence that cybersecurity risks can be managed—even by self-described nontechnical folks. You just need to know where to look.

About the author

E.J. Yerzak, CISA, CISM, CRISC
Director of Cybersecurity Services
Compliance Solutions Strategies (CSS) /
Ascendant Consulting Services

E.J. assists advisers to hedge funds, private equity funds, funds of funds, pension advisers, and retail investment advisers in bridging the gap between compliance and cybersecurity risk management. In addition to conducting compliance program annual reviews, risk assessments, and mock exams, E.J. is the director of Cyber IT Services of the technology team at CSS, which provides cybersecurity consulting services to its clients. In this capacity, E.J. assists firms in assessing and managing their cybersecurity risk, from network vulnerability scanning and penetration testing to onsite cybersecurity assessments and assistance in implementing the NIST Cybersecurity Framework.

E.J. has authored articles and alerts on emerging regulatory and technology issues, and is regularly requested to speak as a cybersecurity expert at industry conferences and events throughout the country. He is a Certified Information Systems Auditor (CISA®), Certified Information Security Manager (CISM®), and Certified in Risk and Information Systems Control (CRISC™).

E.J. holds a Bachelor of Arts in both English and computer science, magna cum laude, from Colgate University; a Master of Science degree in computer information technology from Central Connecticut State University; and a J.D., magna cum laude, from Quinnipiac University School of Law. He is licensed to practice at the State Bar of Connecticut and in federal court before the U.S. District Court for the District of Connecticut.

Online compliance resources

The Schwab Advisor Center compliance page includes additional Compliance Review papers to assist you.

Schwab works with third-party firms to provide select resources that help keep you informed of certain regulatory and compliance developments. Access *Compliance Hot Topics*, templates and guideline documents, archived issues of *Compliance Review*, and third-party resources. These resources are complimentary and exclusive to advisors who work with Schwab Advisor Services™.

(0525-UZ43) NWS108530Q2CY-01 (05/25)

charles SCHWAB

Own your tomorrow®