Evolving Cybersecurity Expectations: The SEC Proposes its First Comprehensive Cyber and Data Security Rules

By Amber Allen and Craig Watanabe

About the Authors:

Amber Allen is VP and General Counsel with Fairview Cyber, LLC and Fairview Investment Services, LLC. She may be reached at amber.allen@fairviewinvest.com.

Craig Watanabe is the Director of IA Compliance at DFPG Investments. He may be reached at cwatanabe@dfpg.com.

On February 9th, 2022, the SEC proposed its first comprehensive cyber and data security rules, Rule 206(4)-9 under the Advisers Act and Rule 38a-2 under the Investment Company Act (the "Proposed Cyber Rules"). The Proposed Cyber Rules codify the requirement for advisers to maintain comprehensive cybersecurity policies and procedures and adhere to certain disclosure and recordkeeping requirements. Historically, the SEC relied on Regulations S-ID and S-P, Risk Alerts, IM Guidance, and various enforcement actions to set expectations for advisers to establish reasonably designed cyber security policies and procedures. The Proposed Cyber Rules not only increase existing responsibilities, but seemingly reflect a change in rulemaking methodology at the Commission, moving from principles-based regulations to rules-based requirements. This article: (1) discusses the evolution of the SEC's cybersecurity expectations, reviewing the principles-based regulations of the past and the Proposed Cyber Rules; and (2) serves as a planning guide for firms to evaluate the steps necessary to prepare for compliance with the Proposed Rule. Please see the Cybersecurity Tool Kit included at the end of the article (and in the NSCP Resource Library), including:

- Appendix A: Template Cybersecurity Policies and Procedures
- Appendix B: Template Cybersecurity Testing Module
- Appendix C: Cybersecurity Readiness Assessment
- Appendix D: IT Vendor Due Diligence Questionnaire

Please note that at the time of publication, the Proposed Rule is subject to change and, while unlikely, could possibly be withdrawn. The tools incorporate the Proposed Rules but are still instructive with the understanding that certain provisions are subject to change.

The Evolution of the SEC's Cybersecurity Expectations

Regulatory History of Cybersecurity: It is important to be familiar with current rules and guidance since none of the rules or guidance have been withdrawn. Much of the guidance has been codified in the Proposed Rule so the past guidance remains helpful.

Regulation S-ID: The Federal Trade Commission (FTC) began enforcing its Fair and Accurate Credit Transactions Act of 2003 (FACT Act) Red Flags Rule in January 2011.[1] Shortly thereafter, the SEC and CFTC were assigned responsibility for rulemaking and enforcement of identity theft red flag rules through the Dodd-Frank Wall Street Reform and Consumer Protection Act. In 2013, the SEC and CFTC jointly issued Regulation S-ID, which is aimed at preventing and detecting identity theft.[2] Under Regulation S-ID, financial institutions, including many investment advisers, that maintain "covered accounts" must identity, detect, and prevent identity theft. Advisers have leeway in crafting policies and procedures to fit the needs of their firms, so long as these elements are met.

Regulation S-P: Congress enacted the Gramm, Leach, Bliley Act (GLBA) in November 1999 and in response the SEC Enacted Regulation S-P in June 2000 (commonly referred to as "Reg S-P"). Many in the industry associate Reg S-P with privacy, often neglecting the "S", which stands for safeguards. Reg S-P, Rule 30(a) is foundation of all cybersecurity regulation for SEC registrants. It is principles-based and only one small section (see below Rule 30(a) in its entirety).

> **§ 248.30 Procedures to safeguard customer records and information; disposal of consumer report information.**
>
> (a) Every broker, dealer, and investment company, and every investment adviser registered with the Commission must adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. These written policies and procedures must be reasonably designed to:

1. *See* Identity Theft Red Flags Rule, U.S. Securities and Exchange Commission (April 19, 2013) available at: https://www.finra.org/rules-guidance/key-topics/customer-information-protection/ftc-red-flags-rule
2. Ibid.

(1) Ensure the security and confidentiality of customer records and information;
(2) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
(3) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

Broad-based principles regulations, such as Rule 30(a), are informed by speeches, Risk Alerts, no-action letters and enforcement precedent. The SEC offered its first Risk Alert on cybersecurity on April 15, 2014[3] (as further discussed below) and there have been numerous Risk Alerts since then on cybersecurity. Moreover, the SEC has highlighted cybersecurity in each of its annual Examination Priorities letters since 2014. It is noteworthy that there have been no no-action letters on cybersecurity.

The inaugural cybersecurity enforcement action by the SEC was against R.T. Jones Capital Equities Management on September 22, 2015[4] and there have since been numerous enforcement actions for violations of Rule 30(a).

Finally, many States have enacted cybersecurity regulations to protect citizens under their jurisdiction. A full discussion of State regulation is beyond the scope of this article.

Risk Alerts: With minimal requirements in place under Regulation S-ID and Regulation S-P, the Commission used various Risk Assessments and Guidance, rather than rulemaking, to establish expectations.

In April 2014, the SEC added cybersecurity to its list of annual priorities (as part of its focus on trading). Shortly thereafter, it issued a risk alert on its cybersecurity initiative in 2014[5]. As part of the initiative, the Division of Examinations (the "Division") conducted examinations focused on:
- Cybersecurity governance;
- Identification and assessment of cybersecurity risks;
- Protection of networks and information;
- Risks associated with remote customer access and funds transfer requests;
- Risks associated with vendors and other third parties; and
- Detection of unauthorized activity, and experiences with certain cybersecurity threats.

In February 2015, the Division published a summary of its examination observations during the 2014 Cybersecurity Initiative[6]. A few months later, the SEC's Division of Investment Management issued *IM Guidance* in April 2015, encouraging advisers to address cybersecurity risk as it relates to identity theft and data protection, fraud, and business continuity, as well as other disruptions in service.

In September 2015, the Division issued a Risk Alert to announce another exam sweep[7] focused on:
- Governance and Risk Assessment;
- Access Rights and Controls;
- Data Loss Prevention;
- Vendor Management;
- Training; and
- Incident Response.

3. *See* "OCIE Cybersecurity Initiative", Risk Alert Volume IV, Issue 2, U.S Securities and Exchange Commission, Office of Compliance Inspections and Examinations (April 15, 2014) available at: Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf.
4. *See* "In the Matter of R.T. Jones Capital Equities Management, Inc.", Administrative Proceeding File No. 3-16827 (September 22, 2015) available at: R.T. Jones Capital Equities Management, Inc. (sec.gov).
5. *See* "OCIE Cybersecurity Initiative", Risk Alert Volume IV, Issue 2, U.S Securities and Exchange Commission, Office of Compliance Inspections and Examinations (April 15, 2014) available at: Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf.
6. *See* "Cybersecurity Examination Sweep Summary", Office of Compliance Inspections and Examinations (February 3, 2015), available at: Risk Alert: Cybersecurity Examination Sweep Summary.
7. *See* "OCIE's 2015 Cybersecurity Examination Initiative", Office of Compliance Inspections and Examinations (September 15, 2015), available at: OCIE's 2015 Cybersecurity Examination Initiative

In August 2017, the Division issued a National Exam Program Risk Alert which outlined its observations from recent Cybersecurity Examinations[8]. Though its observations included a number of items where firms had made progress, the Division noted the following issues:

- Policies and procedures were not reasonably tailored because they provided only general guidance, were narrowly scoped, or were vague and did not articulate procedures for implementing the policies.
- Firms did not appear to adhere to or enforce policies and procedures, or the policies and procedures did not reflect the firms' actual practices.
- Regulation S-P-related issues among firms that did not appear to adequately conduct system maintenance, such as the installation of software patches to address security vulnerabilities.
- Risk assessments were not regularly conducted or were outdated.

Proposed Rule 206(4)-9 Cybersecurity Risk Management

Rather than describe the rules, we think it is more helpful to see the rules through to implementation. Template Cybersecurity Policies and Procedures are attached as an appendix to this article and are also available in the NSCP Resource Library.

Proposed Rule 206(4)-9 requires that firms have written policies and procedures governing cybersecurity. The good news is virtually all of the requirements of the Rule merely elevate prior guidance, so there is really nothing new. The new requirements, as further described below, establish certain required disclosures and reporting (Rules 204-3 and 204-6).

Many firms already have cybersecurity policies and procedures, either in a dedicated chapter of the compliance manual or in various other chapters such as privacy. If using the template provided, firms should conduct thorough reviews of their existing cybersecurity policies and procedures to maintain alignment and eliminate redundancy.

Governance and Risk Assessments

Good governance is critical. In a speech to the Northwestern Pritzker School of Law on January 24, 2022[9], SEC Chair Gary Gensler quoted Jen Easterly, Director of the Cybersecurity and Infrastructure Agency, in saying, "cybersecurity is a team sport." One of the first steps in cybersecurity is to define who is on the team and who are the captains. The template policy and procedures include a table to list key players in the cybersecurity team, which generally includes Compliance, IT and Senior Management.

The SEC has been advocating for cybersecurity risk assessments since it began focusing on cybersecurity in 2014. Unlike other regulators, such as the NY Department of Financial Services (NY DFS), the SEC is requiring risk assessments but left wide latitude in how the risk assessments are performed. There is a tremendous difference between a self-assessment and a comprehensive vulnerability assessment or penetration test by a qualified information security consultant. There is also a huge difference between a one-person RIA and a large Wall Street institution. One size does not fit all.

Cybersecurity risk assessments are highly beneficial and the first decision firms must make is how to approach the risk assessment. Factors that weigh into the decision are the size of the firm (in terms of number of users), budget and complexity of the network and IT infrastructure. A critical consideration is the internal capability of the firm to perform a meaningful self-assessment. Should a firm want to perform a self-assessment, there is a Cybersecurity Readiness Assessment in the NSCP Resource Library, which can be used as a guide.

8. *See* "Observations from Cybersecurity Examinations", Office of Compliance Inspections and Examinations (August 7, 2017), available at: Risk Alert: Observations from Cybersecurity Examinations.
9. *See* "Cybersecurity and Laws" speech by Chair Gary Gensler at the Northwestern Pritzker School of Law (January 24, 2022) available at: SEC.gov | Cybersecurity and Securities Laws.

User Security and Access

The Proposed Rules codify prior guidance and do not materially change user security and access requirements. However, it is noteworthy that a downside of prescriptive regulation is that rules become outdated. 206(4)-9 will now require that firms utilize multi-factor authentication (MFA). However, user security and access controls are evolving. For example, Windows 11 is the first Microsoft operating system that has a hardware requirement. The hardware is the Trusted Platform Module (TPM) which is a security chip embedded on the motherboard. The TPM acts as a second form of very robust hardware authentication, thus Windows 11 will have native MFA in what Microsoft calls "chip to cloud security."

There is a significant human element in cybersecurity. It is estimated that 70% of breaches entail a compromised user. The policies and procedures template includes acceptable use policies and requires user awareness training, which is the key to addressing the human element of cybersecurity.

Information Protection

It is helpful to address information protection as "data in motion" and "data at rest." Rule 206(4)-9 does not make this distinction, but protecting data in motion usually entails secure email. Protecting data at rest has become native in most systems today. The key to information protection is encryption and most data at rest today is encrypted by default, except email.

One of the best cyber defenses is maintain up-to-date hardware and software. Cyber attacks are constantly evolving, but so are cyber defenses which are incorporated in the latest hardware and software. While not required under 206(4)-9, the template policies attached include a policy to create an aged inventory of hardware and software and develop an upgrade policy. In the past, upgrade cycles ranged from 6-8 years, at which time the older hardware/software started to suffer usability and functionality issues. However, when considering security, upgrade cycles should be about half of that period (or 3-4 years). While a 4 year-old computer is still functional, it is not as secure as a new computer.

Vendor Management

In 2021 SecureLink and the Ponemon Institute jointly released a white paper, "A Crisis in Third-Party Remote Access Security"[10] which included survey results that 44% of respondents had experienced breaches in the past 12 months and 74% of those cited it was the result of giving too much privileged access to third-parties. The SEC has issued guidance that consistently advises firms to perform robust due diligence on IT vendors and now this guidance has been codified in a formal rule proposal. Vendor management is a significant risk and it is imperative that robust due diligence be performed initially and on an ongoing basis.

Vendor due diligence reviews can be a challenge for firms to conduct for a variety of reasons, from unresponsive vendors to lack of expertise in-house. If your firm lacks expertise or time to conduct vendor reviews internally, consider outsourcing the review to another service provider. If your firm conducts vendor reviews in-house, there is an IT Vendor Due Diligence Questionnaire (DDQ) in the NSCP Resource Library. Firms that experience difficulty obtaining the necessary information should consider requesting the vendor provide a redacted DDQ they have recently completed, along with the vendor's policies and procedures, including a BCP and information security to supplement your efforts. This is easy for the vendor and will provide most the information needed to complete the assessment.

10. *See* "A Crisis in Third-Party Remote Access Security" by SecureLink and the Ponemon Institute (May 4, 2021) available at: A Crisis in Third-Party Remote Access Security (securelink.com).

Finally, firms should review vendor contracts for breach notification, indemnification clauses and data access. Data access is important to back up a firm's books and records and critical when changing vendors. Firms should negotiate a contractual right to obtain a copy of the firm's data. Additionally, when possible, include language in the agreement that requires the vendor to respond to reasonable due diligence requests annually.

Cybersecurity Threat and Vulnerability Management

Most victims of cyberattacks were informed by law enforcement or the hacker[11]. Most hackers are very adept at sidestepping intrusion detection and the average time to detect a breach is 191 days, which is eons in cyber time[12]. Intrusion detection monitoring is an expensive, but necessary, control.

The SEC has repeatedly issued guidance that firms should have a written incident response plan (IRP) and this has now been codified in proposed Rule 206(4)-9. The IRP has a lot in common with a BCP, and it is important for firms to undertake robust measures before memorializing the plan. With regard to the IRP, many small firms will include their managed IT service provider as the key player. However, many managed IT service providers lack the capability to respond to significant incidents, since incident response is outside of their day-to-day scope of services. Further, many managed IT service providers are unfamiliar with legal and regulatory requirements. Firms should consider the advisability of retaining remediation specialists. Typically, the best remediation specialists are dealing with breaches daily and are in constant communication with law enforcement. They will have better intelligence that enables them to better handle the incident. For a small to medium firm that has a remediation specialist on retainer, this will be the key player in the IRP.

A second and underappreciated element of the IRP is cyber liability insurance. Cyber liability insurance has great utility beyond the financial benefits. Once coverage is invoked, the insurer assumes the financial risk and has a vested interest to manage and mitigate the risk. Certain cyber policies will cover the cost of remediation specialists and legal counsel, so be sure to review your policy before engaging these vendors.

If a firm has cyber liability insurance and a remediation specialist and legal counsel on retainer, then documenting the IRP is fairly straightforward.

Amended Rule 204-3 Delivery of Brochures and Brochure Supplements

The SEC defined numerous terms and one of the key definitions is:

> "*Cybersecurity incident*" means an unauthorized occurrence on or conducted through an adviser's information systems that jeopardizes the confidentiality, integrity, or availability of an adviser's information systems or any adviser information residing therein."

This definition is extremely broad and does not include a de minimis. The SEC revised the instructions for Form ADV Part 2A to include Item 20:

> "Item 20. Cybersecurity Risks and Incidents
>
> A. Risks. Describe the cybersecurity risks that could materially affect the advisory services you offer. Describe how you assess, prioritize, and address cybersecurity risks created by the nature and scope of your business.

11. *See A Tale of Two Cities*: https://en.wikiquote.org/wiki/A_Tale_of_Two_Cities (with apologies to Charles Dickens).
12. *See A Tale of Two Cities*: https://en.wikiquote.org/wiki/A_Tale_of_Two_Cities (with apologies to Charles Dickens).

B. Incidents. Provide a description of any cybersecurity incident that that has occurred within the last two fiscal years that has significantly disrupted or degraded your ability to maintain critical operations, or has led to the unauthorized access or use of adviser information, resulting in substantial harm to you or your clients. The description of each incident must include the following information to the extent known: the entity or entities affected; when the incident was discovered and whether it is ongoing; whether any data was stolen, altered or accessed or used for any other unauthorized purpose; the effect of the incident on the adviser's operations; and whether the adviser, or service provider, has remediated or is currently remediating the incident."

Item 20 is a new requirement and will be the most onerous element of the new rules for many firms. It is also likely to receive numerous comments because, if adopted as written, it would require firms to disclose ongoing breaches, increasing the firm's cybersecurity risk of subsequent or add-on attacks at an already vulnerable time.

Proposed Rule 204-6 Cybersecurity Incident Reporting

A second new element of the rules is mandatory reporting under proposed Rule 204-6(1) on the new Form ADV-C:

> "Report to the Commission any *significant adviser cybersecurity* incident or significant fund cybersecurity incident, promptly, but in no event more than 48 hours, after having a reasonable basis to conclude that any such incident has occurred or is occurring by filing Form ADV-C electronically on the Investment Adviser Registration Depository (IARD).
>
> *Significant adviser cybersecurity incident* means a cybersecurity incident, or a group of related cybersecurity incidents, that significantly disrupts or degrades the adviser's ability, or the ability of a private fund client of the adviser, to maintain critical operations, or leads to the unauthorized access or use of adviser information, where the unauthorized access or use of such information results in: (1) Substantial harm to the adviser, or (2) Substantial harm to a client, or an investor in a private fund, whose information was accessed."

Again, this rule is very broad and 204-6(2) will require Form ADV-C to be amended within 48 hours under certain conditions.

Amended Rule 204-2 Cybersecurity Books and Records

The rules described above mandate certain written polices, disclosures, and reporting. Amended Rule 204-2 requires firms to maintain these new required records consistent with other books and records.

Annual Review

In a slew of proposed rulemaking, the SEC proposed an amendment to Rule 206(4)-7, requiring all advisers to document their annual reviews in writing. The proposed Rule 206(4)-9 requires annual review of the cybersecurity policies and procedures. Most firms will meet this requirement by folding it into the 206(4)-7 annual review. To aid in this process, there is a Cybersecurity Testing Template aligned with the template policies and procedures in the NSCP Resource Library.

Conclusion

While the majority of the Proposed Rules merely elevate and codify existing guidance, firms should not underestimate the potential updates that may be necessary to comply with the proposal. Firms that are not already complying with best practices would likely have significant updates to make if the proposed rules are adopted as proposed. The finalization of the proposals seems likely, and these proposed changes are major. To aid firms in updating their compliance programs, NSCP has developed helpful tools including the Cybersecurity Policies and Procedures Template, Cybersecurity Testing Template, Cybersecurity Readiness Assessment, and the IT Vendor Due Diligence Questionnaire. ■

Appendix A: Template Cybersecurity Policies and Procedures

A. INTRODUCTION

In February 2022 the SEC proposed Rules under the Investment Adviser's Act of 1940 to enhance cybersecurity.

- New Rule 206(4)-9 requires comprehensive written policies and procedures
- New Rule 204-6 requires cybersecurity incident reporting
- Amended Rule 204-3 requires cybersecurity disclosures in Form ADV, specifically, the SEC has added Form ADV Part 2A, Item 20 – Cybersecurity Risks and Incidents
- Amended Rule 204-2 requires records pertaining to 206(4)-9

Cybersecurity is a significant risk and this section of the manual memorializes the policies, procedures and controls **XYZ** has implemented to address cyber threats.

B. DEFINITIONS

- *Adviser information* means any electronic information related to the adviser's business, including personal information, received, maintained, created, or processed by the adviser.
- *Adviser information* systems means the information resources owned or used by the adviser, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of adviser information to maintain or support the adviser's operations.
- *Cybersecurity incident* means an unauthorized occurrence on or conducted through an adviser's information systems that jeopardizes the confidentiality, integrity, or availability of an adviser's information systems or any adviser information residing therein.
- *Cybersecurity risk* means financial, operational, legal, reputational, and other consequences that could result from cybersecurity incidents, threats, and vulnerabilities.
- *Cybersecurity threat* means any potential occurrence that may result in an unauthorized effort to adversely affect the confidentiality, integrity, or availability of an adviser's information systems or any adviser information residing therein.
- *Cybersecurity vulnerability* means a vulnerability in an adviser's information systems, information system security procedures, or internal controls, including vulnerabilities in their design, configuration, maintenance, or implementation that, if exploited, could result in a cybersecurity incident.
- *Personal information means*:
    - Any information that can be used, alone or in conjunction with any other information, to identify an individual, such as name, date of birth, place of birth, telephone number, street address, mother's maiden name, Social Security number, driver's license number, electronic mail address, account number, account password, biometric records or other nonpublic authentication information; or
    - Any other non-public information regarding a client's account.
    - Note: Some States have different definitions.

- *Significant adviser cybersecurity incident* means a cybersecurity incident, or a group of related cybersecurity incidents, that significantly disrupts or degrades the adviser's ability, or the ability of a private fund client of the adviser, to maintain critical operations, or leads to the unauthorized access or use of adviser information, where the unauthorized access or use of such information results in:
    - Substantial harm to the adviser, or
    - Substantial harm to a client, or an investor in a private fund, whose information was accessed.
- *Significant fund cybersecurity* incident has the same meaning as in 270.38a-2 of this chapter (rule 38a-2 under the Investment Company Act of 1940).

C. CYBERSECURITY WRITTEN POLICIES AND PROCEDURES

New Rule 206(4)-9 requires cybersecurity policies and procedures. As a means reasonably designed to prevent fraudulent, deceptive, or manipulative acts, practices, or courses of business within the meaning of section 206(4) of the Act (15 U.S.C. 80b6(4)), it is unlawful for any investment adviser registered or required to be registered under section 203 of the Investment Advisers Act of 1940 (15 U.S.C. 80b-3) to provide investment advice to clients unless the adviser adopts and implements written policies and procedures that are reasonably designed to address the adviser's cybersecurity risks.

In a speech delivered to the Northwestern Pritzker School of Law on January 24, 2022, SEC Chair Gary Gensler described cybersecurity as "team sport." The following is a list of key players in XYZ's cybersecurity **<Complete the table below>**:

Title	Responsibilities
Chief Compliance Officer	
Director of IT	
Managed IT Service Provider	
Remediation Specialist	
Infosec Consultant	
Cyber Insurance Agent	

The written policies and procedures below are intended to satisfy the requirement of Rule 206(4)-9.

D. PROCEDURES

1. Cybersecurity Risk Assessment

a) **XYZ** must perform periodic assessments of cybersecurity risks associated with adviser information systems and adviser information residing therein, including requiring the adviser to:
   (1) Categorize and prioritize cybersecurity risks based on an inventory of the components of the adviser information systems and adviser information residing therein and the potential effect of a cybersecurity incident on the adviser; and
   (2) Identify the adviser's service providers that receive, maintain, or process adviser

information, or are otherwise permitted to access adviser information systems and any adviser information residing therein, and assess the cybersecurity risks associated with the adviser's use of these service providers.

(3) Require written documentation of any risk assessments.

b) Describe whether you perform internal or external risk assessments and stipulate approximately how often. For NSCP members there are self-assessment templates in the Resource Library. An important consideration in deciding to perform a self-assessment is the knowledge and expertise you have internally.

c) Ideally the deliverable when the risk assessment is completed will be an actionable list of risk and remedial steps to be taken. Describe your process for addressing the follow up to the risk assessment. Typically, IT will have a significant role in the implementation.

d) **XYZ** will maintain documentation of all cybersecurity risk assessments and remedialsteps taken.

2. User Security and Access

a) **XYZ** must implement controls designed to minimize user-related risks and prevent unauthorized access to adviser information systems and adviser information residing therein, including:

(1) Requiring standards of behavior for individuals authorized to access adviser information systems and any adviser information residing therein, such as an acceptable use policy (see below).

(2) Identifying and authenticating individual users, including implementing authentication measures that require users to present a combination of two or more credentials for access verification.

(3) Establishing procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication.

(4) Restricting access to specific adviser information systems or components thereof and adviser information residing therein solely to individuals requiring access to such systems and information as is necessary for them to perform their responsibilities and functions on behalf of the adviser; and

(5) Securing remote access technologies.

b) Acceptable Use Policies

(1) Supervised Persons *must*:

(a) Take reasonable precautions to protect **XYZ**'s systems and data.

(b) Access files, data, and protected records only if you are authorized do to so or if the information is publicly available.

(c) Contact IT if there is doubt concerning your authorization to access any **XYZ** IT resource.

(d) Take care to protect passwords that are used to access the firm's systems.

(i) It is recommended that you use strong passwords (must include at least 12 characters and three of the following: number, lower case letter, upper case letter, or symbol).

(ii) Update or reset your password at least once every six months.

(iii) NEVER share passwords with any individual for any reason.

(iv) User access may be blocked after multiple unsuccessful login attempts.

(e) Be vigilant to potential phishing attacks:

(i) Take reasonable steps to confirm the identity of any client or other authorized person requesting client nonpublic information before providing such information; and

(ii) Take reasonable steps to confirm the identity of individuals and the security or authenticity of any websites before providing company confidential information, including but not limited to, account numbers and passwords.

(f) Guard against access to files and take precautions to protect Information Technology (IT) devices when you are away from the workstation, including logging off or locking computers or other devices.

(g) Only use software furnished by **XYZ**. Under certain circumstances, you may use software if it has first been approved by IT and/or the third party IT provider.

(h) Contact the CCO or other authorized person if you need to transfer data from **XYZ**'s system.

(i) When using an external storage media or other device to transfer data:

(i) The device used must be a **XYZ**-approved device.

(ii) Employee purchased media, or those containing personal information, must not be connected to **XYZ** equipment at any time.

(iii) External media must be encrypted and password protected.

(iv) Employees should not store **XYZ** business related data external media. All **XYZ** business related data must be stored on the company's network drive.

(v) If **XYZ** network connection is unavailable (ex: training outside of **XYZ**), external media may be used for short-term data storage and back-up purposes only if approved by **XYZ**.

(j) Report the following instances to the CCO:

(i) Receiving or obtaining information to which you are not entitled (Note: the owner or sender of such information must also be notified);

(ii) Becoming aware of breaches in security;

(iii) Becoming aware of any theft or loss of information;

(iv) Becoming aware of any inappropriate use of company-provided IT resources; or

(v) Becoming aware of any violations of these policies.

(2) Supervised Persons must *not*:

(a) Knowingly commit security violations. This includes one or more of the following:

(i) Accessing records within or outside the computer and communications facilities for which you are not authorized.

(ii) Copying, disclosing, transferring, examining, re-naming, or changing information or programs belonging to another user unless given express permission to do so by the user responsible for the information or programs.

(iii) Violating the privacy of individual users by reading e-mail or private communications unless you are specifically authorized to maintain and support the system.

(b) Knowingly or recklessly spread computer viruses. To reduce this threat, you may not import files from unknown or questionable sources.

(c) Transfer personally identifiable information through electronic transmission, other than facsimile, to a person outside of the secure system of the business, unless **XYZ** uses encryption to ensure the security of the transmission.

(i) It is not a violation of this policy to transmit the last four digits of a social security number or publicly available information that is lawfully made available to the general public.

c) There is a significant human element to cybersecurity which is addressed through training. **XYZ** must perform and document regular initial and ongoing user awareness training. Training is also indicated any time there is a change in the firms systems and after a cyber incident.
d) Passwords are said to be the "weakest link" of cybersecurity. Multi-factor authentication (MFA) requires at least two forms of authentication such as a security token in addition to the username and password. The three critical use cases for MFA are securing computer logins, the file server and email accounts. **XYZ** must implement MFA. <describe the form(s) of MFA at **XYZ**.>
e) Remote access to the **XYZ** network must be secured via a VPN and MFA.
f) Upon termination of personnel, IT will immediately change any passwords that could be used to access firm systems or client accounts on a remote basis. This includes individual as well as firm-wide passwords.

3. Information Protection

a) **XYZ** must implement measures designed to monitor adviser information systems and protect adviser information from unauthorized access or use, based on a periodic assessment of the adviser information systems and adviser information that resides on the systems. These measures must take into account:
   (1) The sensitivity level and importance of adviser information to its business operations;
   (2) Whether any adviser information is personal information;
   (3) Where and how adviser information is accessed, stored and transmitted, including the monitoring of adviser information in transmission;
   (4) Adviser information systems access controls and malware protection; and
   (5) The potential effect a cybersecurity incident involving adviser information could have on the adviser and its clients, including the ability for the adviser to continue to provide investment advice.

b) One of the best cyber controls is to establish a hardware/software upgrade cycle that takes security into account. Cyber attacks are constantly evolving but so are cyber defenses. These defenses are only available on newer hardware/software. **XYZ** should create an aged inventory of all hardware/software and establish an upgrade policy.

4. Vendor Management

a) **XYZ** must perform oversight of service providers that receive, maintain, or process adviser information, or are otherwise permitted to access adviser information systems and any adviser information residing therein and through that oversight document that such service providers, pursuant to a written contract between the adviser and any such service provider, are required to implement and maintain appropriate measures, including the practices described in paragraphs (a)(1), (a)(2), (a)(3)(i), (a)(4), and (a)(5) of this section, that are designed to protect adviser information and adviser information systems.

b) **XYZ** will follow established procedures using the IT Vendor Due Diligence Questionnaire and document each initial and ongoing review.

5. Cybersecurity Threat and Vulnerability Management

a) **XYZ** must take measures to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to adviser information systems and the adviser information residing therein;
b) Cybersecurity incident response and recovery.
   (1) Require measures to detect, respond to, and recover from a cybersecurity incident, including policies and procedures that are reasonably designed to ensure:
   (2) Continued operations of the adviser;
   (3) The protection of adviser information systems and the adviser information residing therein;
   (4) External and internal cybersecurity incident information sharing and communications; and
   (5) Reporting of significant cybersecurity incidents under Rule 204-6 (17 CFR 275.204- 6).
   (6) Require written documentation of any cybersecurity incident, including the adviser's response to and recovery from such an incident.
c) **XYZ** should implemented cyber policy auditing software that secures and monitors each endpoint device.
d) **XYZ** has a written Incident Response Plan which will be referenced in response to a cyber incident.
e) As part of the incident response plan, **XYZ** has a remediation specialist on retainer who will be contacted as needed.
f) **XYZ** has retained cyber liability insurance. The claim will be filed promptly in response to a cyber incident.

6. Cybersecurity Incident Reporting

a) For purposes of this policy, "security breach" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by **XYZ**. Good faith acquisition of personal information by an employee or agent of **XYZ** for the purposes of **XYZ** is not a security breach, provided that the personal information is not used or subject to further unauthorized disclosure.
b) **XYZ** must report to the Commission any significant adviser cybersecurity incident or significant fund cybersecurity incident, promptly, but in no event more than 48 hours, after having a reasonable basis to conclude that any such incident has occurred or is occurring by filing Form ADV-C electronically on the Investment Adviser Registration Depository (IARD);
c) **XYZ** must amend any previously filed Form ADV-C promptly, but in no event more than 48 hours after:
   (1) Any information previously reported to the Commission on Form ADV-C pertaining to a significant adviser cybersecurity incident or a significant fund cybersecurity becoming materially inaccurate;
   (2) New material information pertaining to a significant adviser cybersecurity i incident or a significant fund cybersecurity incident previously reported to the Commission on Form ADV-C being discovered; or
   (3) Any significant adviser cybersecurity incident or significant fund cybersecurity incident being resolved or any internal investigation pertaining to such an incident being closed.

7. Cybersecurity Books and Records

a) **XYZ** must create and retain:
   (1) A copy of the investment adviser's policies and procedures formulated pursuant to 275.206(4)-7(a) and 206(4)-9 that are in effect, or at any time within the past five years were in effect.
   (2) A copy of the investment adviser's written report documenting the investment adviser's annual review of the cybersecurity policies and procedures conducted pursuant to 275.206(4)-9(b) in the last five years.
   (3) A copy of any Form ADV-C, and amendments filed by the adviser under 275.204-6 in the last five years.
   (4) Records documenting the occurrence of any cybersecurity incident, as defined in 275.206(4)-9(c), occurring in the last five years, including records related to any response and recovery from such an incident.
   (5) Records documenting any risk assessment conducted pursuant to the cybersecurity policies and procedures required by 275.206(4)-9(a)(1) in the last five years.

8. Delivery of Brochures and Brochure Supplements

a) Form ADV Part 2A must be amended to include Item 20 – Cybersecurity Risk and Incidents.
b) **XYZ** must deliver the following to each client promptly after a brochure or brochure supplement, as applicable, has been amended if the amendment:
   (1) Adds disclosure of an event or incident, or materially revises information already disclosed about an event or incident: in response to Item 9 of Part 2A of Form ADV or Item 3 of Part 2B of Form ADV (Disciplinary Information), or Item 20.B of Part 2A of Form ADV (Cybersecurity Risks and Incidents).
   (2) Relates to the change in disciplinary information or information about a significant cybersecurity incident.
   (3) Includes a statement describing the material facts relating to the change in disciplinary information or information about a significant cybersecurity incident.

9. Annual Review

a) **XYZ** must review and assess the design and effectiveness of the cybersecurity policies and procedures required by paragraph (a) of this section, including whether they reflect changes in cybersecurity risk over the time period covered by the review; and
b) **XYZ** must prepare a written report that, at a minimum, describes the review, the assessment, and any control tests performed, explains their results, documents any cybersecurity incident that occurred since the date of the last report, and discusses any material changes to the policies and procedures since the date of the last report.
c) **XYZ** will incorporate these requirements into the 206(4)-7 Annual Review.

IMPORTANT NOTE: This document contains sample language that is just an example and is for general educational and informational purposes. It does not constitute a legal opinion or legal advice that may be relied on by third parties and should not be construed as advice, recommendations or suggestions. Users should consult their own legal counsel for information on what should be contained in the document based on their individual circumstances and should consider substituting their own language where appropriate. Further, this sample is based on the law in effect as of February 2022. Changes may have occurred in the law since this sample was prepared. As a result, users should consult with legal advisers to determine if there have been any relevant developments since them. ■

Appendix B: Template Cybersecurity Testing Module

As a Registered Investment Advisor, your firm is subject to SEC Rule 206(4)-9 and Reg S-P, Rule 30

(i) Implement written policies and procedures designed to protect non-public Client records in a secure manner;
(ii) Implement procedures to comply with required incident reporting
(iii) Include Item 20 – Cybersecurity Risks and Incidents in Form ADV Part 2A
(iv) Maintain required books and records relating to cybersecurity

Key Question	Answer	Compliment (if Applicable)
Governance and Risk Assessment		
Have you implemented written cybersecurity policies and procedures in accordance with 206(4)-9?		
Does the firm have procedures to update and deliver Form ADV Part 2A, Item 20 as required under 206(4)-9?		
Has your firm established cybersecurity governance policies identifying responsible parties and their roles?		
Has your firm performed a cybersecurity vulnerability assessment? Has your firm performed a penetration test?		
Does the firm have procedures requiring a formal annual review of the design and effectiveness of the Cybersecurity policies and procedures?		
Access Controls		
Does the firm utilize robust access controls such as multifactor authentication on critical information assets, such as computer logins, the file server and email accounts?		
Has the firm implemented procedures for change management, including procedures for terminating access when employees separate service?		
Does the firm limit access based on role?		
Data Protection		
Has the firm classified information and restricted access to necessary users?		
Has the firm secured remote access to the firm's network?		
Has the firm created an aged inventory of all hardware and software?		
Does the firm have a policy regarding hardware and software upgrades?		
Does the firm utilize methods for protecting data-in-motion such as secure email?		
Does the firm have cybersecurity policies for remote office and remote employees?		
Incident Response		
Does the firm have a written Incident Response Plan?		
Does the firm have procedures to report cyber incidents to the SEC on Form ADV-C?		
Does the firm have cyber liability insurance?		
User Awareness and Training		
Has the firm implemented written Acceptable Use policies?		
Does the firm conduct user awareness training?		
Vendor Due Diligence		
Does the firm perform initial and ongong due diligence on IT Service Providers?		
Does your firm conduct initial and ongoign due diligence on key vendors?		

Appendix C: Cybersecurity Readiness Assessment

OCIE's 2015 Cybersecurity Examination Initiative[1]

The SEC Office of Compliance Inspections and Examinations ("OCIE") is following up the 2014 cybersecurity sweep examinations with a second round of examinations in 2015. The 2015 sweep examination request letter asks more penetrating questions than the 2014 sweep letter. This Readiness Assessment has converted the 2015 sweep letter into a tool Firms can use to assess their cybersecurity readiness. Practical guidance is provided to help firms understand and achieve tangible improvements in their ability to defend against cyber attacks.

Rating Scale

4 – Fully Implemented	The item has been fully implemented and documented.
3 – Mostly Implemented	The item is more than 50% implemented. Plans may exist for further implementation or the firm may deem the actions to date are adequate.
2 – Partially Implemented	The item is less than 50% implemented. Plans may exist for further implementation or the firm may deem the actions to date are adequate.
1 – Not Implemented	The firm has not implemented this practice. Plans may exist for future consideration.
N/A	The issue is not relevant to the firm.

1.0 Goverance and Risk Assessment

Item	Issue	Rating	Rating Rationale	Plan of Action
1.1	The Firm has policies and procedures to protect customer information including those designed to secure customer information, protect against anticipated threats and protect against unauthorized access to customer accounts or information.		*[In the wake of the RT Jones Capital case, having cybersecurity policies and procedures should be considered essential]*	
1.2	The Firm has patch management policies that address the prompt installation of critical patches and documentation of such actions.		*[Auto-updates should be enabled]*	

1. *See* "OCIE's 2015 Cybersecurity Examination Initiative," Securities and Exchange Commission National Exam Program Risk Alert by the Office of Compliance Examinations and Inspections, Volume IV, Issue 8, (September 15, 2015) available at http://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

1.3	The Firm provides the Board and Senior Management briefing materials regarding cyber-related risks, cybersecurity incident response planning, actual cybersecurity incidents, and cybersecurity-related incidents involving vendors.			
1.4	The Firm has identified the person responsible for the cybersecurity program, has clearly defined the role and provided the resources to implement the program.			
1.5	The Firm has identified the organizational structure, particularly the positions and departments responsible for cybersecurity related matters and where they fit within the firm's organization or hierarchy.			
1.6	The Firm conducts periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business and compliance consequences and has been responsive to remediate any findings.		*[This Readiness Assessment fulfills this mandate]*	
1.7	The Firm has policies regarding penetration testing and has been responsive to remediate any findings.		*[For small firms penetration testing is not essential]*	
1.8	The Firm performs vulnerability scans and has been responsive to remediate any findings.		*[Vulnerability scans help identify issues with network configuration]*	

2.0 Access Rights and Controls

Item	Issue	Rating	Rating Rationale	Plan of Action
2.1	The Firm has policies and procedures establishing employee access rights, including the employee's role or group membership.		*[Heeding the principle of least permissions, it is highly recommended to have a permissions hierarchy]*	
2.2	The Firm has policies and procedures for updating or terminating access rights based on personnel or system changes.		*[This should be addressed in the policies under "Change Management"]*	

2.3	Management approval is required for changes to access rights or controls.			
2.4	The Firm documents the tracking of employee access rights, changes to those access rights, and any manager approvals for those changes.			
2.5	The Firm maintains information related to former employees' last date of employment and the date their access to the firm's systems was terminated.			
2.6	The Firm maintains information related to current employees who have been reassigned by the firm to a new group or function, including their date of reassignment and the date their access to the firm's systems was modified.			
2.7	The Firm maintains documentation of the systems or applications for which the firm uses multi-factor authentication for employee and customer access as well as documentation evidencing implementation of any related policies and procedures and information on systems or applications for which the firm does not use multi-factor authentication.		*[Multi-factor authentication is economical and very effective. Multi-factor authentication is highly recommended.]*	
2.8	The Firm has policies and procedures related to log-in attempts, log-in failures, lockouts, and unlocks or resets for perimeter-facing systems and information regarding the process the firm uses to enforce these policies and procedures and to review perimeter-facing systems for failed log-in attempts, deactivation of access, dormant user accounts, and unauthorized log-in attempts.			
2.9	The Firm documents instances in which system users, including employees, customers, and vendors, received entitlements or access to firm data, systems, or reports in contravention of the firm's policies or practices or without required authorization as well as information related to any remediation efforts undertaken in response.			

2.10	Firm has policies and procedures regarding system notifications to users, including employees and customers, of appropriate usage obligations when logging into the firm's system (e.g., log-on banners, warning messages, or acceptable use notifications) and sample documentation evidencing implementation of these policies and procedures.			
2.11	Firm has policies and procedures regarding devices used to access the firm's system externally (i.e., firm-issued and personal devices), including those addressing the encryption of such devices and the firm's ability to remotely monitor, track, and deactivate remote devices.		*[The Firm must affirmatively identify and secure each access point to the network. This is referred to as endpoint protection.]*	
2.12	The Firm documents customer complaints received by the firm related to customer access, including a description of the resolution of the complaints and any remediation efforts undertaken in response.			
2.13	Firm has policies and procedures related to verification of the authenticity of customer requests to transfer funds.		*[Telephonic verifications is nearly universally required. Verifications should be performed on third-party and same-name transfers. Banks do not check the name on wire transfer requests, only the account number and routing number. Some fraudulent wire requests are formatted to look like same-name transfers.]*	
2.14	The Firm documents any reviews of employee access rights and restrictions with respect to job-specific resources within the network and any related documentation.			
2.15	The Firm documents any internal audit conducted by the firm that covered access rights and controls.			

3.0 Data Loss Prevention

Item	Issue	Rating	Rating Rationale	Plan of Action
3.1	The Firm has mapped data, with particular emphasis on understanding information ownership and how the firm documents or evidences personally identifiable information ("PII").			
3.2	The Firm has addressed the systems, utilities, and tools used to prevent, detect, and monitor data loss as it relates to PII and access to customer accounts, including a description of the functions and source of these resources.		*[Heeding the principle of defense in depth, a system that employs multiple layers of encryption is very robust. The second layer is typically disk or file encryption. Data encryption is economical and effective. It is highly recommended.]*	
3.3	The Firm has policies related to data classification, including: information regarding the types of data classification; the risk level (e.g., low, medium, or high) associated with each data classification; the factors considered when classifying data; and how the factors and risks are considered when the firm makes data classification determinations.			
3.4	The Firm has policies and procedures related to monitoring exfiltration and unauthorized distribution of sensitive information outside of the firm through various distribution channels (e.g., email, physical media, hard copy, or web-based file transfer programs) and any documentation evidencing this monitoring.			

4.0 Vendor Management

Item	Issue	Rating	Rating Rationale	Plan of Action
4.1	Comprehensive due diligence with regard to vendor selection is performed initially, and on a periodic basis.		*[If a firm has undergone an internal controls audit, the report (SSAE16, SOC-1, SOC-2) will be very helpful]*	
4.2	The Firm reviews contracts, agreements, and the related approval process.		*[Key contract provisions include the confidentiality clause and data ownership]*	
4.3	The Firm has policies and procedures for the supervision, monitoring, tracking, and access control of vendors.			
4.4	The Firm maintains any risk assessments, performance measurements and reports required of vendors.			
4.5	The Firm maintains documentation regarding third-party vendors with access to the firm's network or data, including the services provided and contractual terms related to accessing firm networks or data.			
4.6	The Firm maintains information regarding third-party vendors that facilitate the mitigation of cybersecurity risks by means related to access controls, data loss prevention, and management of PII, including a description of the services each vendor provides to the firm and contractual terms included in vendor contracts involving cybersecurity-related services.			
4.7	The Firm maintains information regarding written contingency plans the firm has with its vendors concerning, for instance, conflicts of interest, bankruptcy, or other issues that might put the vendor out of business or in financial difficulty.			
4.8	The Firm retains sample documents or notices required of third-party vendors, such as those required prior to any significant changes to the third-party vendors' systems, components, or services that could potentially have security impacts to the firm and the firm's data containing PII.			

5.0 Training

Item	Issue	Rating	Rating Rationale	Plan of Action
5.1	Training is provided by the firm to its employees regarding information security and risks. Documentation includes the training method (e.g., in person, computer-based learning, or email alerts); dates, topics, and groups of participating employees; and any written guidance or materials provided.		*[According to the 2015 Verizon Data Breach Investigations report, two-thirds of breaches involved a compromised user. People are the weakest link but user awareness training can be highly effective and is strongly recommended]*	
5.2	Training is provided by the firm to third-party vendors or business partners related to information security.			

6.0 Incident Response

Item	Issue	Rating	Rating Rationale	Plan of Action
6.1	The Firm has policies and procedures or the firm's business continuity of operations plan that address mitigation of the effects of a cybersecurity incident and/or recovery from such an incident, including policies regarding cybersecurity incident response and responsibility for losses associated with attacks or intrusions impacting clients.		*[Identify a remediation company now instead of during a time of crisis]*	
6.2	The Firm has a process for conducting tests or exercises of its incident response plan, including the frequency of, and reports from, such testing and any responsive remediation efforts taken, if applicable.			
6.3	The Firm documents system-generated alerts related to data loss of sensitive information or confidential customer records and information, including any related findings and any responsive remediation efforts taken.			
6.4	The Firm documents incidents of unauthorized internal or external distributions of PII, including the date of the incidents, discovery process, escalation, and any responsive remediation efforts taken.			
6.5	The Firm documents successful unauthorized internal or external incidents related to access, including the date of the incidents, discovery process, escalation, and any responsive remediation efforts taken.			

Appendix D: IT Vendor Due Diligence Questionnaire

A. VENDOR INFORMATION

1. General Information

Firm Name: _____

Firm Address: _____

Contact Name(s):_____

Phone: _____ Email: _____ Website: _____

2. Is the vendor owned/controlled by a Parent Co.? ☐ Yes ☐ No

3. Personnel:
   Approximate # of employees: _____
   Does the vendor hire independent contractors? ☐ Yes ☐ No

4. Background Information:
   How many years has the vendor been in business? _____
   How many years has the vendor provided the outsourced function? _____
   Is the vendor known to the Firm or employees of the Firm? ☐ Yes ☐ No
   If yes, please name the individual(s) and describe any prior experience each had with the vendor:

5. Has the vendor been involved in any litigation or formal regulatory action? ☐ Yes ☐ No
   If yes, please provide a brief summary of each incident.

B. POLICIES AND PROCEDURES

6. Please provide a copy of your policies and procedures that address:
   a. Acceptable use of firm infrastructure and data
   b. Account management
   c. Anti-virus protection
   d. Change management
   e. Data backup and data loss prevention
   f. Secure email
   g. Encryption policy
   h. Incident response
   i. Network access
   j. Password policy
   k. Patch management
   l. Physical security
   m. Portable computing

n. Privacy policy
o. User awareness training
p. Vendor access
q. Procedures for addressing non-compliance

7. Do you outsource any information security functions (if so provide details)?

8. Please provide all procedures for compliance with privacy laws and regulations related to maintaining the protection of customer data?
9. Please identify the senior staff member(s) responsible for:
   a. User awareness training
   b. Policy enforcement
   c. Risk evaluation
   d. Risk mitigation
   e. Regulatory compliance

C. INFORMATION SECURITY ADMINISTRATION

10. Please provide the most recent internal controls report (SSAE 16, SOC-1 or SOC-2.)
11. Please provide details of the firm's policy for conducting vulnerability assessments.
12. Please provide details of the firm's policy for conducting penetration tests.
13. Please describe limits to administrator level access on network and systems infrastructure.
14. Please list any professional certifications held by your Information Security staff.
15. What is the average tenure of your information security staff?
16. How is access to security logs controlled (i.e. firewall logs, etc.)?

D. DISASTER RECOVERY AND BUSINESS CONTINUITY

17. Please provide a copy of your business continuity plan.
18. Do you have redundant public utilities connections? (Please describe)
19. Do you employ UPSs, generators, etc.? (Please describe)
20. Do you employ fire and flood detection and suppression systems? (Please describe)
21. Please describe the testing procedures for disaster recovery.
22. Are manual backup/restore procedures documented and practiced in case of automatic backup failure?
23. Can you meet recovery time objectives (RTO) and recovery point objectives (RPO) for all products and services contracted?

To avoid redundancy in the following sections please note if any items are addressed in material already requested such as cybersecurity policies & procedures, internal controls reports or the business continuity plan.

E. PHYSICAL SECURITY

24. Please describe the access controls at your data center location(s):
    a) Token/Cards:
    b) Key Pad Controls:
    c) Biometric Controls:
    d) Guards:
    e) Other:

25. How is access to the data center monitored and logged?
26. Do you monitor and escort visitors through critical parts of your company? (Please describe)
27. Do you maintain visitor logs for more than 30 days? (Please describe)

F. NETWORK CONFIGURATION

28. Are all routers configured with access control to allow only authorized traffic in the network?
29. Do you ensure default passwords are changed on networking devices?
30. Do you control the change frequency and distribution of admin access to network infrastructure?
31. Do you use the most current encryption protocol (currently WPA2) for your wireless network?

G. PATCH MANAGEMENT

32. Are all your networking devices at the latest patch level?
33. Do you have an automated patch management solution deployed?
34. Do you have a procedure to keep track of announcement of vulnerability patches for your networking devices?
35. Are any of your software applications non-supported and must be patched manually (if so provide details)?

H. REMOTE ACCESS

36. Are there any remote access control methods available to access your network including:
    a. Call backs
    b. PKI
    c. RADIUS/TACACS
    d. User ID/Password
    e. Token bases access control
    f. Other
37. Do you allow admin functions to be performed over unencrypted external links?
38. Do you review audit logs on remote access?

I. FIREWALL AND INTRUSION DETECTION MONITORING

39. Do you have a security team that keeps track of all known vulnerabilities?
40. Do you have a perimeter scanning/monitoring systems in place?
41. Do you have an Intrusion Detection Monitoring System implemented (if so provide details)?
42. Do you employ the following intrusion detection methods:
    a. HIDS
    b. NID:
    c. Honey Pots
    d. Rogue device and services detection
43. Do you have an Incident Response Team?
44. Do you employ a firewall server(s) to protect your network?

45. Do you have any other applications (e.g. DNS) running on the same firewall server? (Please describe)
46. Do you allow non-standard (>1024) IP ports to pass through your firewall?
47. Have you scanned and verified all the allowable services provided by your firewall server?
48. Do you use firewall-reporting tools to analyze your firewall log?
49. Do you protect your internal IP address range(s) (i.e., use NAT/RFC 1918)?
50. Do you log successes and failures to access?

J. ANTI-VIRUS PROTECTION

51. Do you scan all emails for viruses?
52. Is there explicit policy requiring anti-virus software on networked computers?
53. Do you have centralized administration of virus control, such as distribution of signature updates, reporting, and policy enforcement and vendor management? (Please describe)
54. Is there a system for automated scanning of external software installed on your network? (Please describe)
55. Does the virus checking software run in the background with established frequency of scanning, etc.?
56. Are end-users prevented from disabling anti-virus software on network computers?
57. Do you allow installation of personal and non-corporate approved software on network computers?

K. ACCESS CONTROL

58. How will data be secured at your site?
59. Will data be accessible from the Internet?
60. Who will have access to data?
61. How do you prevent other clients from accessing data?
62. How and where are user IDs and passwords stored and secured?
63. Will the access credentials be encrypted when passing through public network?
64. Do you employ any mechanisms that facilitate secure data exchange?

We realize that responding to due diligence questionnaire's ("DDQ") such as this can be tedious and we appreciate your cooperation. The key documents we request are: your information security policies & procedures, internal controls report and business continuity plan. If possible, we would appreciate providing these documents as soon as possible so that we may begin performing our due diligence right away. Thank you in advance for your cooperation. ■