




**Schulte Roth & Zabel**

# **Information Security: Obligations and Expectations**

A White Paper by Jason S. Kaplan, Robert R. Kiesel, Holly H. Weiss  
and Michael L. Yaeger

**May 2015**





Information security is not only a good idea — it is also a legal obligation. Federal and state laws impose obligations on businesses, including investment advisers, to keep their data secure. Most of these laws focus on requiring businesses to take reasonable security measures. While it may take regulators and courts years to clearly define what exactly those are, best practices that facilitate compliance can and should be developed and followed now. This *White Paper* outlines information security issues that businesses need to address, from complying with the SEC’s recent Risk Alert concerning the OCIE’s cybersecurity policy examinations to handling human resources and insurance concerns.

## Table of Contents

I.	Introduction	1
II.	The SEC’s Risk Alert	2
III.	The NIST Framework: Why It Matters and What It Is	3
IV.	Becoming Compliant: Where to Start	4
V.	Practical Cybersecurity: Human Resources Policies and Insider and Third-Party Risk	6
VI.	Data Breaches	12
VII.	Insurance	14
	Endnotes	16
	Authors	18

## I. Introduction

### A. “Reasonable” Cybersecurity

Information security is not only a good idea — it’s a legal obligation. There are federal and state laws that impose obligations on businesses, including investment advisers, to keep their data secure. Most of these laws can be summarized as follows: Take reasonable security measures. What are reasonable security measures? It may take the regulators and courts years to reach a definitive answer (if they ever do), but there are best practices that facilitate compliance.

### B. Existing Rules

1. Investment advisers must maintain data security not only because they may be obligated to do so by contract (e.g., under contracts between the firm and investors or commercial vendors), to comply with fiduciary obligations, or for practical business reasons (e.g., to protect trade secrets), but also for compliance reasons — namely, the existence of federal and state statutes and regulations that require data security. There are two essential types of data security obligations: (1) the duty to protect information; and (2) the duty to disclose breaches.
  - (a) The Duty to Protect: provide reasonable security for data, systems and communications.
  - (b) The Duty to Disclose: disclose breaches to affected parties and regulators, and disclose material risks.
2. Right now, the applicable laws are mostly concerned with protecting the personally identifiable information of human beings (e.g., social security numbers or addresses) (“PII”).
3. At present, 47 states (and Washington, D.C.; Puerto Rico; Guam; and the Virgin Islands) have data protection laws concerning protection of individuals’ PII (all states other than Alabama, New Mexico and South Dakota). (The National Conference of State Legislatures provides a list of the relevant laws.)<sup>1</sup>

### C. Sector-Specific Laws: the Gramm-Leach-Bliley Act

1. The two most significant existing federal regulations for investment advisers and investment companies focus on protecting customers’ PII.
  - (a) Section 30 of Regulation S-P: Requires brokers, dealers, investment companies and registered investment advisers to adopt written policies and procedures designed to protect “customer records and information.”<sup>2</sup> The protections are expected to be “administrative, technical, and physical” and require board approval.
  - (b) Regulation S-ID, the Identity Theft Red Flags Rules: Require covered entities to develop and implement a written program to “detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.”<sup>3</sup>

2. The Securities and Exchange Commission (the “SEC”) has brought enforcement cases against firms for violating Regulation S-P by failing to follow or enforce cybersecurity policies and procedures.<sup>4</sup>
3. Regulations S-P and S-ID are also enforced against broker-dealers by the Financial Industry Regulatory Authority (“FINRA”) in accordance with FINRA’s supervision rules requiring that member firms comply with applicable securities laws and rules.<sup>5</sup> Entities not regulated by FINRA should look to FINRA’s enforcement cases because they may be used as persuasive, non-binding authority.<sup>6</sup>
4. SEC staff expect registered investment advisers to adopt and maintain written information security policies (each a “WISP”). Question 2 of the SEC’s Office of Compliance Inspections and Examinations (“OCIE”) Risk Alert (described below) requires an investment adviser to provide a copy of its policy to OCIE.

## II. The SEC’s Risk Alert

### A. The Sweep

1. In April 2014, the OCIE issued a Risk Alert announcing that it would be “conducting examinations of more than 50 registered broker-dealers and registered investment advisers, and that the exams will focus on areas related to cybersecurity.”<sup>7</sup>
2. To help registrants and their compliance professionals prepare for these examinations, OCIE included an appendix to the Risk Alert containing a seven-page “sample” cybersecurity document request. The document request is the most substantive part of the Risk Alert and merits close reading. Taken together, the questions suggest that OCIE is building upon existing regulations that concern risks to customers’ PII and will now also assess firms’ vulnerability to cybersecurity risks in general, including “misappropriation of funds, securities, sensitive ... Firm information, or damage to the Firm’s network or data.”
3. In other words, the data at issue is no longer just PII. It could be, for example, trading strategies or algorithms. The SEC is interested in all the risks that misuse of technology may pose to a firm’s assets, including the firm’s reputation.
4. Topics addressed in the Risk Alert include:
  - (a) Cybersecurity governance;
  - (b) Identification and assessment of cybersecurity risks;
  - (c) Protection of networks and information;
  - (d) Risks associated with remote customer access and funds transfer requests;
  - (e) Risks associated with vendors and other third parties with access to the firm’s networks, customer data or other sensitive information;
  - (f) Detection of unauthorized activity;

**OCIE is building upon existing regulations that concern risks to customers’ PII**

(g) Experiences with certain cybersecurity threats; and

(h) Cyber risk insurance.

The sample request is quite broad and covers a great deal of material in 28 multi-part questions. At the same time, some questions seek precise information on narrow issues, such as the particular dates since Jan. 1, 2013 of any security incidents, including “the service affected, and the nature and length of the impairment.”<sup>8</sup>

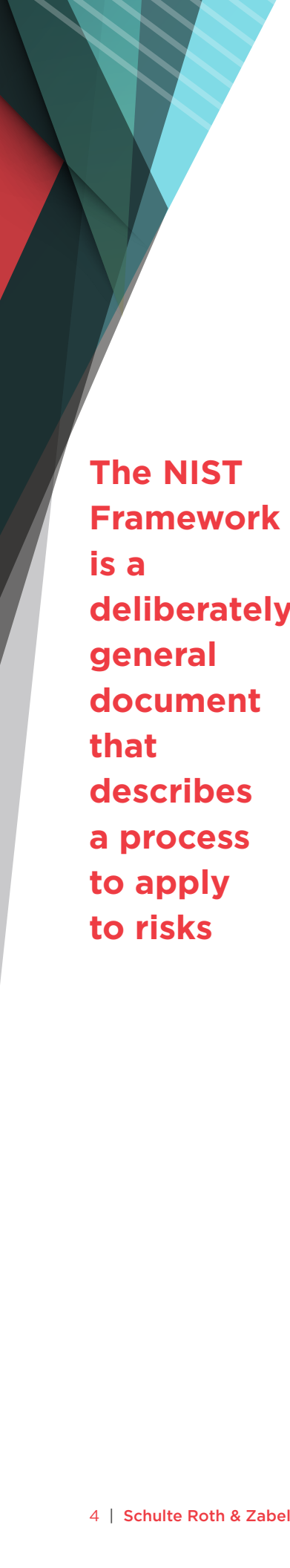
5. A firm’s WISP should address as many of the applicable issues raised by the Risk Alert as possible.
6. On Feb. 3, 2015, the OCIE issued another Risk Alert, summarizing the SEC’s findings from the examinations conducted under the first Risk Alert.<sup>9</sup>

### III. The NIST Framework: Why It Matters and What It Is

#### A. Why the NIST Framework Matters

The SEC’s questions in the Risk Alert give hints about what “reasonable security measures” might be by guiding firms toward the adoption of a published standard such as the one published by the National Institute of Standards and Technology (“NIST”), discussed below.

1. The Risk Alert expressly states that some of the questions track information outlined in the “Framework for Improving Critical Infrastructure Cybersecurity,” released on Feb. 12, 2014 by NIST.<sup>10</sup>
2. Moreover, one question in the appendix specifically asks the registrant to “identify any published cybersecurity risk management process standards that the entity has used to model its information security architecture and processes [on], such as those issued by NIST or the International Organization for Standardization (ISO).”
3. NIST is a part of the U.S. Commerce Department, and the Framework is the product of a collaboration between the government and the private sector. The Framework is designed to “provid[e] a consensus description of what’s needed for a comprehensive cybersecurity program.”<sup>11</sup> It compiles, and makes reference to, similar past frameworks that other organizations, such as COBIT and ISO, have developed.
4. Further, the SEC has pointed to the Framework in places other than the Risk Alert. In a June 2014 speech, one of the SEC Commissioners, Luis Aguilar, suggested that the Framework may be a baseline for best practices by companies, including in assessing legal or regulatory exposure to cyber risks. “At a minimum,” he stated, “boards should work with management to assess their corporate policies to ensure how they match-up to the Framework’s guidelines — and whether more may be needed.”<sup>12</sup>
5. A firm is not required to use the Framework to develop its security plan, but the Framework has been highlighted by the SEC and thus it is not lightly ignored.



**The NIST Framework is a deliberately general document that describes a process to apply to risks**

B. The Nature of the Framework

1. The Framework is a deliberately general document that describes a process to apply to risks. It does not prescribe particular tools or products, such as firewalls or encryption. The generality of the document is a little frustrating, but probably essential. It is designed to be flexible enough to accommodate technology and business change.
2. The Framework consists of three parts: the Framework Core, the Framework Profile and the Framework Implementation Tiers.
  - (a) “The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors.”<sup>13</sup> These activities are organized into five functions — Identify, Protect, Detect, Respond and Recover. “When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization’s management of cybersecurity risk”<sup>14</sup> and allow an organization to learn from past security incidents.
  - (b) “The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a ‘Current’ Profile (the ‘as is’ state) with a ‘Target’ Profile (the ‘to be’ state). ... Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.”<sup>15</sup>
    - (i) For example, a Profile can aid communication with vendors and other third parties who have authorized access to a firm’s systems or information. A firm with a Profile has something to show its vendor, making it easier to describe what needs to be protected, and what a vendor must do before it will be granted access. Similarly, a firm could request that the prospective vendor submit its own Profile.
  - (c) The Framework Implementation Tiers range from Partial (Tier 1) to Adaptive (Tier 4). They describe: (1) “an increasing degree of rigor and sophistication in cybersecurity risk management practices”; (2) the extent to which cybersecurity risk management is informed by business needs”; and (3) the extent to which cybersecurity risk management is “integrated into an organization’s overall risk management practices.”<sup>16</sup> In determining what Tier they desire, firms should determine which level meets the firm’s goals and “is feasible to implement.”<sup>17</sup>

**IV. Becoming Compliant: Where to Start**

A. Firm-Level Risk Assessments

1. OCIE expects that firms will maintain a detailed inventory and understanding of their cyber infrastructure. This includes physical devices, the software platforms and applications used on the network, network resources, connections and “data flows (including locations where customer data is housed).”<sup>18</sup>

2. The SEC is concerned with firms' vulnerability to cybersecurity risks in general, including "misappropriation of funds, securities, ... [and] Firm information[.]"<sup>19</sup> Managers should accordingly review existing related policies, such as controls on processing redemption requests and IT safeguards, in a cybersecurity context.
3. Every fund manager should be prepared to explain how it designed and maintains its infrastructure, its incident response plan and its training for employees. Third-party security firms can assist in this effort.
4. Consider doing a gap analysis. Discover where the gaps in the firm's security are and close them.
  - (a) A gap analysis is an analysis of what you have done, where you are now, and where you want to go.
    - (i) "What you have done" includes any previous security reviews or audits.
    - (ii) "Where you are now" includes any existing personnel, policies, procedures and controls you currently have in place. A full risk assessment identifying all systems, all "treasure" (what you want to protect), all risks and all residual risks after the controls are applied.
    - (iii) "Where you want to go" means identifying any regulatory compliance needs, selecting an appropriate framework (e.g., NIST; ISO 27001) and developing a roadmap for hiring, policy development, control implementation, ongoing risk assessment, etc.
  - (b) The gap analysis should be done at the firm level, but also at lower levels within the firm. At the firm level, guidance is provided to the entire firm and is applicable to all types of information systems and mission objectives, and a standard risk threshold exists. Different groups at a fund manager will likely present different types of information security risks (e.g., investor relations and trading).

## B. Cybersecurity Personnel

Many of OCIE's questions in the Risk Alert focus as much on the "who" as the "what." Firms should have well-defined roles and responsibilities for cybersecurity personnel, and to that end should designate a chief information security officer, or the functional equivalent — an employee in charge of information security as distinct from IT operations. Question 21 in particular asks for considerable detail regarding which specific persons (identified by title, department and job function) are responsible for tasks such as detecting malware, "maintaining baseline information about expected events on the Firm's network," and "monitoring the activity of third party service providers with access to the Firm's network." Compliance personnel should be familiar with the division of labor in the technology department.

**Almost every aspect of a firm's existence intersects with computers and digital data**

C. Records of Cybersecurity Incidents

1. Firms should maintain detailed records relating to cybersecurity incidents. This is one of the more significant parts of the Risk Alert. Financial firms of course have long-standing obligations to maintain accurate books and records, but such record-keeping is not traditionally associated with cybersecurity or even technology support departments. OCIE is not asking firms to catalogue tech support tickets; it is seeking granular detail on particular security incidents, both retrospectively and going forward. For example, Question 24 asks for details on many kinds of cybersecurity events, such as the detection of malware on a firm's devices, or the impairment of a "critical Firm web or network resource [due to] a software or hardware malfunction." This may require a considerable expansion of current record-keeping, and collaboration between cybersecurity and legal compliance personnel. The Risk Alert does not expressly address what makes a particular incident material, but Question 24 hints that the SEC will recognize materiality concerns in some way because it allows respondents to omit some incidents that: (1) resulted in losses of \$5,000 or less; (2) did not result in "unauthorized access to customer information"; or (3) did not make a firm service unavailable for "more than 10 minutes."<sup>20</sup>
2. In designing their record-keeping system, cybersecurity personnel might also consider additional uses for the records beyond complying with OCIE's document requests. The records created in response to OCIE's request could also become a valuable tool for firms to use in their own internal investigations, or to assist firms if they become the victims of tortious or criminal conduct. For example, the malware used to misappropriate data can sit on a server for months before it is detected, and thus the investigation of a breach may be aided by examining seemingly unconnected events several months or even years prior. Valuable investigative resources such as log records (e.g., web server access logs and secure shell server logs) can be overwritten or deleted, so preserving the kind of information requested by OCIE in a readily accessible form may prove useful.

D. Disaster Recovery

Managers should review their existing disaster recovery plans to ensure that they are up-to-date with firm operations and that they take into account cybersecurity and identity theft prevention policies. Note that Regulation S-P requires a written business continuity plan.

**V. Practical Cybersecurity: Human Resources Policies and Insider and Third-Party Risk**

A. Human Resources

1. Almost every aspect of a firm's existence intersects with computers and digital data. Accordingly, cybersecurity is less a separate concern than a theme that should run through all of a firm's risk management policies. Personnel policies are no exception.
  - (a) Since the advent of the cellphone, employees have had firm information in the palms of their hands. As cellphones have become smartphones, the amount of firm information that employees have access to at all times has increased exponentially. As Bring-Your-Own-



Device (“BYOD”) practices have spread, the wall between personal and business use has grown thinner. Now, many employees own the devices on which they work, and they engage in both business and personal activities on the same device.


(b) Technological change — in particular the BYOD trend — heightens employee security risks:

- (i) Lost or Stolen Devices: Mobile devices are more likely than desktop computers to be lost or stolen.
- (ii) Cloud-Based Storage: Firm data saved in “cloud” storage by employees may be unsecure and out of the firm’s reach.
- (iii) Wireless (In)security: Data traveling on unsecured wireless networks can easily be stolen.
- (iv) Downloads/Uploads: Malware may cause damage to a firm’s system and threaten its security.
- (v) Friends and Family: Mobile devices may be accessed by friends or family.

## 2. Disgruntled/Disloyal/Terminated Employees

(a) Firm-owned devices, and the business data stored thereon, can readily be secured, studied and wiped by the firm. Most court decisions involving employee challenges to an employer’s access to personal data based on privacy concerns have favored the employer and have turned on the fact that the employer owned the device or system on which the information was stored or transmitted. By contrast, a device owned by an employee that contains personal data may not be readily secured legally. Relevant federal statutes include the Electronic Communications Privacy Act (“ECPA”) and the Computer Fraud and Abuse Act (“CFAA”).

- (i) ECPA: Title I prohibits wiretapping unless there is consent from one party; it is for a legitimate business reason; it is routinely conducted; and, in some federal appellate court circuits, the party is informed that he/she is being monitored. There are exemptions for publicly accessible radio communications, government officials and communication services providers. Title II (the Stored Communications Act (“SCA”)), bans surreptitious access to stored communications like email, social media messages and text messages. The SCA makes it a crime to intentionally access without authorization or exceed an authorization to access stored communications. Therefore, employers may not access an employee’s web-based personal email; nor can they access password-protected social media posts without consent.<sup>21</sup> If the communications pass through firm servers or are stored on firm equipment (e.g., hard drives), however, employers may access personal email and social media posts.<sup>22</sup>

- 
- (ii) CFAA: The CFAA prohibits employers from intentionally accessing a computer without authorization. Employees have sued their employers under the CFAA for accessing the employees' phones, devices or accounts without authorization.<sup>23</sup>
  - (iii) Eighteen states (New Hampshire, Rhode Island, New Jersey, Maryland, Michigan, Illinois, Wisconsin, Tennessee, Louisiana, Missouri, Oklahoma, New Mexico, Colorado, Utah, Nevada, California, Oregon and Washington) have passed so-called "anti-snooping" laws prohibiting employers from demanding passwords to access personal email and social networking sites. There is no federal equivalent yet. New York has several bills pending on the same subject.
- (b) To avoid running afoul of these statutory protections, and to protect firm information, firms should:
- (i) Obtain advance authorization to access and wipe information stored on employee-owned mobile devices that contain firm information;
  - (ii) Consider using mobile management software to, among other things, create a "corporate sandbox" that segregates firm information from personal information (and consider that even though it may be technologically possible to access personal information on a dual-use device, there is a downside to doing so);
  - (iii) Clearly delineate where work cannot be done (e.g., prohibit firm work on personal email accounts); and
  - (iv) Craft policies that ensure that employees do not have an expectation of privacy with respect to firm information on their own devices or personal information transmitted using the firm's technology or stored on the firm's systems.
- (c) Proprietary and Trade Secret Information
- (i) A critical element of proof in a trade secret theft case is that the employer has taken "reasonable measures to protect" the information it claims was misappropriated.<sup>24</sup> The evidentiary burden is difficult to meet when the information walks out the door every day in employees' pockets.
  - (ii) Employees can misappropriate firm information in a variety of ways. For example, they may photograph documents or screens or surreptitiously record discussions, and because smartphones are ubiquitous, the theft may not be obvious. Or, employees may electronically transfer data, using email, internet-based storage or portable storage drives.
  - (iii) To protect firm information, in addition to traditional measures, such as confidentiality agreements and policies, firms should take technical precautions, such as restricting access to trade secret data (e.g., by using proprietary software source code for trading algorithms), disabling transmission of information to

portable drives, encrypting information and compartmentalizing information (so that no single individual can misappropriate a particular trade secret).

(d) Employee Speech Protections


- (i) Recently the National Labor Relations Board (“NLRB”) has been pursuing employers, both unionized and not unionized, challenging overly broad policies that chill employee speech and terminations stemming from employee speech on social media sites.
- (ii) Section 7 of the National Labor Relations Act of 1935 (“NLRA”) gives employees the “right to self-organize, to form, join, or assist labor organizations ... and to engage in other concerted activities ... .” Concerted activity includes speech regarding discontent with an employee’s current employer, including complaints about wages or a tough boss.
- (iii) The NLRB has concluded that a policy banning personal use of business devices chills concerted activity and, therefore, is too broad. The NLRB has also concluded that policies that prohibit employees from saying anything about their employers on social media sites are overly broad.<sup>25</sup> To comply with the NLRA, policies should permit non-excessive personal use of the firm’s systems and limit prohibitions with respect to social media.<sup>26</sup> Policies should, however, prohibit employees from using systems that an employer cannot access (such as personal web-based emails) for business.

(e) Training

Training employees is critical, because many security incidents are the result of employee error or misconduct. The consequences of comingling personal and business data and functions on one device are not intuitive to employees. Many problems are not caused by disgruntled employees acting intentionally. Rather, they are caused by innocent insiders. Training will go a long way toward mitigating the risk.

(f) Elements of a BYOD Policy

- (i) Restrictions: A comprehensive BYOD policy should include provisions regarding password protection, encryption of firm data that is stored on the device, lock or wipe after a certain number of unsuccessful access attempts, restrictions on the source of apps (e.g., only Apple or Google), no friends or family access and no storage of corporate data on remote servers through consumer-grade “cloud” storage services. If a firm chooses to use cloud storage, it should carefully select an enterprise-grade provider that provides better encryption and the ability to monitor and wipe what an employee has stored. Employers should also require immediate reporting of lost or stolen devices, use of mobile management software with remote wiping capabilities and use of passwords with safeguards to prevent hacking and misuse of information on the device.



## Risks to investment advisers from vendors are a major concern of the OCIE

- (ii) **Monitoring:** In addition, employers should alert employees that they have no privacy expectation in firm data on the phone or personal data transmitted using the firm's software installed on the phone (e.g., firm email); firms should get consent to monitor data that is stored, sent from or received on the device; and firms should get consent to remotely wipe firm information if the device is lost or stolen and upon termination of employment.
- (iii) **Coordination with Other HR Policies:** Employers should ensure that BYOD policies do not conflict with other HR policies and specify that any other policies such as EEO, anti-harassment, confidentiality and compliance policies apply to work done on the device.
- (iv) **Provisions Contemplating Termination of Employment:** Security issues are most acute upon termination of employment. Remote-wiping capabilities are especially important in this circumstance. Employers should obtain prior permission to wipe the phone of firm information. Using a corporate cloud service and setting up a corporate "sandbox" for employees to use helps preserve the integrity of firm information, but will not capture all firm data if some continues to be stored on the device itself. Employers should therefore require employees to consent to an inspection of the device during and upon termination of employment.
- (v) **Compliance with Record-Keeping Obligations:** Whether or not a firm has a record-keeping obligation depends on the content of the communication rather than the platform used to communicate. If text messages include communications that relate to recommendations or advice by a registered investment adviser, they are subject to the record-keeping obligations under Rule 204-2 of the Investment Advisers Act.<sup>27</sup> Employers should make sure that they have access to and maintain all information that is subject to record-keeping obligations. In addition, policies should allow for retrieval of employee-owned devices for compliance-related inquiries. It is good practice to maintain separate, work-specific, employer-controlled accounts for employees to use on sites such as LinkedIn if they use those platforms for communicating with clients.

### B. Third-Party Risks: Vendor Management

Risks to investment advisers from third parties, and specifically vendors, are a major concern of the OCIE, according to the Risk Alert. Such third parties include fund administrators, prime brokers, consultants and commercial vendors. Questions 16 through 20 cover the firm's management of third-party vendors, addressing issues regarding cybersecurity risk assessment of vendors, training materials used for vendors, segregation of sensitive data from third-party access and security applied to control remote systems access by vendors.

#### 1. The Diligence Process: Choosing a Vendor

- (a) It is prudent to investigate a proposed vendor and its creditworthiness prior to entering into a contract, especially if the vendor is not a household name.

- (b) Some vendors will not negotiate changes to their agreements. In this situation, discomfort with the vendor's contract provisions can be soothed somewhat if the investment adviser can get comfortable with the vendor's product and the vendor itself. The best source of this due-diligence information is other customers of the vendor. It is routine for vendors to offer customer references. Investment advisers should take advantage of these offers.
- (c) Ask for and review the vendor's written information security program. It is standard practice for the vendor to attach its program as an exhibit to the vendor contract as a contractual commitment of the vendor.
- (d) The vendor should advise what industry standards it follows (such as ISO or NIST).
- (e) The vendor should identify any subcontractors that will have access to sensitive information and should provide diligence material for each subcontractor.
- (f) Ask for and review the vendor's incident response plan.
- (g) The vendor should agree to preserve information consistent with any instructions the firm provides, including any litigation and regulatory holds.


## 2. Contract Provisions

Question 17 of the Risk Alert addresses whether the firm incorporates data security requirements into its vendor contracts. Another SRZ-authored publication includes a fairly comprehensive set of data security-related contract provisions that an investment adviser can try to incorporate into its vendor contracts (and of which it should provide examples to OCIE in response to Question 17).<sup>28</sup> These provisions apply to vendor-hosted software-as-a-service and cloud-based vendor arrangements.

## C. Practical Recommendations

No firm's data will be totally secure, but practical steps can be taken to protect a firm against data breaches:

1. **Employee Training:** The most important defense against phishing attacks is to train employees not to interact with suspicious emails.
2. **Passwords and RSA Security Codes:** Restricting system access to users that belong is an obvious and reasonable requirement.
3. **Email Filters:** Spam filters are a significant block to phishing attacks and malware.
4. **Limitation on Administrative Privileges:** Limiting the number of employees with broad system access limits the damage an intruder can cause once the intruder successfully breaches the firm's security layers.



## Develop an incident response plan before a breach happens

5. Technological Devices: Technological devices such as email sandboxes (which allow email to be checked for malware before they can do damage) and virtual air-gapping (allowing Internet access via a vendor's system without exposing the firm's devices) are expensive and may slow down systems, but they can provide effective security.
6. Limitation on Large Downloads: Restricting flash drive downloads by employees limits information lost through employees.

### VI. Data Breaches

#### A. Incident Response Plan

1. Prepare for the possibility that the firm will be breached or suffer some other kind of violation of its security.
  - (a) Develop an incident response plan before a breach happens. This is better than assembling one after the problem happens at 8:00 p.m. on New Year's Eve.
  - (b) Don't just think of the dramatic stuff. A security incident could be a breach by an outside attacker, but it also includes more prosaic events such as the loss of laptops, mobile phones or RSA keys.
  - (c) Assemble a team that includes various parts of the firm such as:
    - (i) Tech security;
    - (ii) Tech operations;
    - (iii) PR;
    - (iv) Audit; and
    - (v) Legal.Specify points of contact for each department and allocate responsibilities, and distribute the list in a way that it can be accessed in an emergency.
  - (d) Develop responses to the most likely attacks (e.g., phishing and insider threats).
  - (e) Test the response plan — regularly, not just when it is first developed.
  - (f) Update the plan regularly, and when a significant technology change event occurs — such as the switch to a new off-site data center, the implementation of a major new piece of software, etc. Also, re-evaluate the plan after each significant incident.
  - (g) One helpful resource is NIST's Computer Security Incident Handling Guide.<sup>29</sup>

#### B. Reporting

1. When to report a data breach (and what to report about it) is very fact specific. Factors that matter include the nature of the data (e.g., whether it was PII), the residence and number of individuals whose information has been compromised, and whether the data was encrypted.

2. Timing of the disclosure. State laws vary, but typically require that affected persons be notified of PII breaches without unreasonable delay. As discussed below, most states also typically allow for delay due to cooperation with law enforcement.
3. Form of the disclosure. Affected persons should typically be notified by either written notice, electronic notice, or, sometimes, substitute notice. Substitute notice typically consists of a combination of email notification, a message posted on the firm's website and publication in statewide media. Substitute notice is not permissible unless the breached form lacks sufficient contact information for the affected persons, or if the firm can show that notice will cost more than a certain amount (different for different states) or must be provided to a certain number of people (also different for different states). For example, substitute notice is allowed by Maine and New Hampshire if the cost exceeds \$5,000 or the firm must notify more than 1,000 individuals, but other states have thresholds of \$250,000 or 500,000 individuals.
4. There is oftentimes no obligation to report a security breach to the SEC or to prepare any particular document regarding the breach and how the firm addressed it. But an internal breach report, and related documentation, may be useful in demonstrating the firm's efforts to address information security concerns.

#### C. Attorney-Client Privilege and Incident Response

1. Try to protect your deliberations. It will make the substance and outcome of your third-party deliberations better.
2. Merely copying your lawyer on a communication doesn't make it privileged.
3. But if incident response or after-action reports are conducted at the direction of a lawyer, it is more likely that courts will find them to be privileged.

#### D. Evidence Collection

1. Document as much as possible — actions that are performed by IT, conversations with users and system owners regarding the incident, etc.
  - (a) The point is to know what happened when, and what the decision-making process was.
    - (i) This information may help a firm to improve its future responses.
    - (ii) This information may also help protect the firm from second-guessing by litigants. It allows the firm to show that the ultimate solution wasn't the only possible solution, and that the interim theories were reasonable.
2. "Preserve evidence from the incident. Make backups (preferably disk image backups, not file system backups) of affected systems. Make copies of log files that contain evidence related to the incident."<sup>30</sup>

## Getting law enforcement involved usually means diminishing control

3. To the extent possible, preserve evidence in a way that doesn't alert the suspected culprit. For example, think carefully about circulating a litigation hold. Who is in the circle of trust?

### E. Communicating and Working with Law Enforcement

1. Under many state laws, a firm that is cooperating with a criminal investigation may delay its breach disclosure to affected individuals.<sup>31</sup>
2. Some things to consider:
  - (a) If a firm wants to pursue its own litigation, criminal litigation may take precedence. Civil litigation is often (but by no means invariably) stayed when there is a parallel criminal case.<sup>32</sup> So getting law enforcement involved usually means diminishing control.
  - (b) On the other hand, if the firm has had to disclose a breach to affected individuals, the firm may be contacted by the Secret Service or FBI anyway. By taking affirmative steps the firm might keep more control of the situation, or at least keep lines of communication with law enforcement open.
  - (c) Law enforcement has investigatory tools that private firms do not (e.g., search warrants and contacts in international law enforcement).
  - (d) When talking to investigators, a firm has to be accurate, of course. The firm may have to discuss aspects of a hack it has seen but doesn't understand.
  - (e) Get outside counsel involved in dealings with law enforcement.
3. Personal relationships can matter in terms of responsiveness and communicating with law enforcement. This may also determine whether to call the FBI, Secret Service, or a particular U.S. Attorney's Office or state District Attorney's office to ask them to open an investigation.
4. What will law enforcement want?
  - (a) Don't do something that tips off the attacker. That could lead to destruction of evidence, or the creation of new back doors allowing the attacker to come back later.
  - (b) May want assistance with undercover operations.
  - (c) Preserve Evidence: Don't turn off computers — that will result in loss of volatile memory. (It may be OK to disconnect from the Internet. Talk to the tech and security team, and ask law enforcement before you do it.)

## VII. Insurance

The insurance markets now offer cyber risk coverage for data breaches. This coverage is available to investment advisers.

### A. Crime Coverage

Many businesses have crime coverage that will cover theft of funds or tangible property through electronic or cyber fraud. Crime coverage, however, will typically not provide coverage for damages resulting from the loss of



data, unauthorized disclosure of information or systems losses due to a virus or other electronic attack. These types of risks typically are covered only by a cybersecurity risk policy.

#### B. Third-Party and First-Party Liability

In today's market you can expect to find cyber coverage for third-party and first-party liability. Coverage should include protection against claims by customers or investors seeking damages due to disclosure of personal and financial data, allegations of a breach of duty due to the failure to prevent and detect a data breach, and the destruction of critical business records. First-party coverage should include the cost and expenses to investigate and respond to the cyber incident, the destruction of valuable data and software and business interruption.

#### C. The SEC's Risk Alert

Question Number 8 of the SEC's Risk Alert asks if the firm under review has in place a cyber risk insurance policy. If a firm answers "yes" to this question, it is likely that the SEC and FINRA will get more comfort from this than from other factors (and maybe more than is due). It may be assumed by the reviewer that the presence of insurance coverage means that a knowledgeable third party (the insurance carrier) has conducted a thorough investigation of the fitness of the firm's security infrastructure and policies prior to providing coverage. This may or may not be true in reality (depending on the size of the policy and the breadth of coverage), but the inference (or reality) of third-party due diligence could make obtaining an insurance policy a relatively cheap certification of regulatory compliance.

## Endnotes

- <sup>1</sup> See [www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx](http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx).
- <sup>2</sup> 17 C.F.R. § 248.30.
- <sup>3</sup> 17 C.F.R. § 248.201(d)(1).
- <sup>4</sup> See, e.g., Exchange Act Release No. 58515, Admin. Proc. File No. 3-13181 (Sept. 11, 2008), *available at* [www.sec.gov/litigation/admin/2008/34-58515.pdf](http://www.sec.gov/litigation/admin/2008/34-58515.pdf); Exchange Act Release No. 64220, Admin. Proc. File No. 3-14328 (April 7, 2011), *available at* [www.sec.gov/litigation/admin/2011/34-64220.pdf](http://www.sec.gov/litigation/admin/2011/34-64220.pdf); Exchange Act Release No. 60733, Admin. Proc. File No. 3-13631 (Sept. 29, 2009), *available at* [www.sec.gov/litigation/admin/2009/34-60733.pdf](http://www.sec.gov/litigation/admin/2009/34-60733.pdf).
- <sup>5</sup> See NASD Rules 3010 and 3012, and FINRA has also brought enforcement cases.
- <sup>6</sup> See, e.g., FINRA Letter of Acceptance, Waiver and Consent No. 2009019893801 (Nov. 21, 2011); FINRA Letter of Acceptance, Waiver and Consent No. 2010022554701 (April 9, 2012); FINRA Letter of Acceptance, Waiver and Consent No. 2008015299801 (April 9, 2010). All of these letters of acceptance are available at <http://disciplinaryactions.finra.org/>.
- <sup>7</sup> Securities and Exchange Commission, Office of Compliance Inspections and Examinations, Risk Alert: OCIE Cybersecurity Initiative (April 15, 2014) (“Risk Alert”), *available at* [www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert+%2526+Appendix++4.15.14.pdf](http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert+%2526+Appendix++4.15.14.pdf).
- <sup>8</sup> Risk Alert, Appendix, Question 24, at 6.
- <sup>9</sup> See SRZ’s Feb. 4, 2015 *Client Alert*, “SEC Cybersecurity Update: OCIE Risk Alert Provides Insights for Private Fund Managers on SEC Cybersecurity Examinations,” *available at* [www.srz.com/SEC\\_Cybersecurity\\_Update\\_OCIE\\_Risk\\_Alert\\_Provides\\_Insights\\_for\\_Private\\_Fund\\_Managers\\_on\\_SEC\\_Cybersecurity\\_Examinations/](http://www.srz.com/SEC_Cybersecurity_Update_OCIE_Risk_Alert_Provides_Insights_for_Private_Fund_Managers_on_SEC_Cybersecurity_Examinations/).
- <sup>10</sup> National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014) (“the Framework”), *available at* [www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf](http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf).
- <sup>11</sup> Statement by Under Secretary of Commerce for Standards and Technology and NIST Director Patrick Gallagher, *cited in* Press Release, NIST Releases Cybersecurity Framework Version 1.0 (Feb. 12, 2014), *available at* [www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm](http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm).
- <sup>12</sup> Luis Aguilar (SEC Commissioner), Boards of Directors, Corporate Governance and Cyber Risks: Sharpening the Focus, Cyber Risks and the Boardroom Conference, New York Stock Exchange (June 10, 2014), *available at* [www.sec.gov/News/Speech/Detail/Speech/1370542057946](http://www.sec.gov/News/Speech/Detail/Speech/1370542057946).
- <sup>13</sup> The Framework, at 1.
- <sup>14</sup> *Id.* at 4.
- <sup>15</sup> *Id.* at 5.
- <sup>16</sup> *Id.* at 9.
- <sup>17</sup> *Id.*
- <sup>18</sup> Risk Alert, Question 24, at 6.
- <sup>19</sup> *Id.* at 7.
- <sup>20</sup> *Id.* at 6 (“If the response to any one item includes more than 10 incidents, the respondent may note the number of incidents and describe incidents that resulted in losses of more than \$5,000, the unauthorized access to customer information, or the unavailability of a Firm service for more than 10 minutes.”).
- <sup>21</sup> See, e.g., *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008).
- <sup>22</sup> See, e.g., *Front, Inc. v. Khalil*, 2013 N.Y. Misc. LEXIS 3157 (N.Y. Co. 2013).
- <sup>23</sup> See, e.g., *Rajae v. Design Tech Homes, Ltd.*, 2014 U.S. Dist. LEXIS 159180 (S. D. Tex. 2014).
- <sup>24</sup> See *MidAmerica Prods., Inc. v. Derke*, 2013 N.Y. Misc. LEXIS 1211 (N.Y. Co. 2013) (holding that customer information sheets were not a trade secret because “plaintiffs did not take any reasonable measures to guard the secrecy” when anyone in the office with access to the computer had access to the data).
- <sup>25</sup> See *Durham School Servs., L.P.*, 360 N.L.R.B. 85 (2014) (a prohibition on sharing information “related to the company or any of its employees or customers” was overbroad and too vague under the NLRA).
- <sup>26</sup> See *Landry’s Inc.*, No. 32-CA-118213 (N.L.R.B. A.L.J. June 26, 2014) (a policy that urged employees not to post about the company was found not to violate the NLRA because it was not an outright prohibition).
- <sup>27</sup> OCIE, Investment Adviser Use of Social Media, National Examination Risk Alert (Jan. 4, 2012), at 2; see 17 C.F.R. § 275.204-2.

- <sup>28</sup> See Robert R. Kiesel, “Model Cybersecurity Contract Terms and Guidance for Investment Managers to Manage Their Third-Party Vendors,” 1 *Cybersecurity Law Report*, No. 6 (June 17, 2015) available at [www.srz.com/Model\\_Cybersecurity\\_Contract\\_Terms\\_and\\_Guidance\\_for\\_Investment\\_Managers\\_to\\_Manage\\_Their\\_Third-Party\\_Vendors/](http://www.srz.com/Model_Cybersecurity_Contract_Terms_and_Guidance_for_Investment_Managers_to_Manage_Their_Third-Party_Vendors/).
- <sup>29</sup> See Paul Cichonski et al., Computer Security Incident Handling Guide, Special Publication 800-61, Revision 2 (August 2012), available at <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>.
- <sup>30</sup> *Id.*, Appendix G, at 68.
- <sup>31</sup> See, e.g., Cal. Civ. Code § 1798.82(c); Conn. Gen. Stat. Ann. § 36a-701b(d); Fla. Stat. Ann. § 817.5681(3); Mass. Gen. Laws Ann. Ch. 93H, § 4; N.Y. Gen. Bus. Law § 899-aa(4); and Tex. Bus. & Com. Code Ann. § 521.053(d).
- <sup>32</sup> See Milton Pollack, *Parallel Civil and Criminal Proceedings*, 129 F.R.D. 201 (S.D.N.Y. 1989); *Parker v. Dawson*, No. 06-CV-6191 JFB WDW, 2007 WL 2462677 (E.D.N.Y. Aug. 27, 2007); *S.E.C. v. Boock*, No. 09 CIV. 8261 (DLC), 2010 WL 2398918 (S.D.N.Y. June 15, 2010); but see *S.E.C. v. Saad*, 384 F. Supp. 2d 692 (S.D.N.Y. 2005) (Rakoff, J.).

## Authors



### Jason S. Kaplan

Partner  
+1 212.756.2760  
jason.kaplan@srz.com



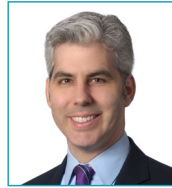
### Holly H. Weiss

Partner  
+1 212.756.2515  
holly.weiss@srz.com



### Robert R. Kiesel

Partner  
+1 212.756.2008  
robert.kiesel@srz.com



### Michael L. Yaeger

Special Counsel  
+1 212.756.2290  
michael.yaeger@srz.com

## About SRZ's Cybersecurity Group

Schulte Roth & Zabel's Cybersecurity Group works with the world's top alternative asset managers, financial institutions and companies operating across a broad range of industries in managing the risks associated with data protection and privacy laws. We advise on obligations under the full range of federal requirements, from HIPAA to Sarbanes-Oxley, as well as state breach notification and other laws. Additionally, we provide advice in connection with the review and purchase of cyber risk insurance products. The Group includes lawyers from multiple practice areas who assist clients on all types of legal and business issues related to cybersecurity, from employment law and bank regulatory requirements to intellectual property and mergers and acquisitions transactions. By closely monitoring proposed regulations and emerging data security laws worldwide, we keep clients abreast of developments that are crucial to running a compliant business, and we also assist with any enforcement and litigation matters related to cybersecurity threats and concerns.

This information has been prepared by Schulte Roth & Zabel LLP ("SRZ") for general informational purposes only. It does not constitute legal advice, and is presented without any representation or warranty as to its accuracy, completeness or timeliness. Transmission or receipt of this information does not create an attorney-client relationship with SRZ. Electronic mail or other communications with SRZ cannot be guaranteed to be confidential and will not (without SRZ agreement) create an attorney-client relationship with SRZ. Parties seeking advice should consult with legal counsel familiar with their particular circumstances. The contents of these materials may constitute attorney advertising under the regulations of various jurisdictions.

© 2015 Schulte Roth & Zabel LLP. All Rights Reserved.



**Schulte Roth&Zabel**  
New York | Washington DC | London  
[www.srz.com](http://www.srz.com)