Data Protection and Collection: Cybersecurity, Insurance and Data Scraping

Schulte Roth&Zabel

25TH ANNUAL

PRIVATE INVESTMENT FUNDS SEMINAR

JANUARY 19, 2016

Partner
New York Office
+1 212.756.2760
jason.kaplan@srz.com

Practices

Investment Management
Hedge Funds
Private Equity
Regulatory & Compliance

Jason S. Kaplan

Jason's practice concentrates on corporate and securities matters for investment managers and alternative investment funds. He represents institutional and entrepreneurial investment managers, financial services firms and private investment funds in all aspects of their business. He advises managers of hedge, private equity and hybrid funds regarding the structure of their businesses and on day-to-day operational, securities, corporate and compliance issues; structures and negotiates seed and strategic investments and relationships and joint ventures; and advises investment managers with respect to regulatory and compliance issues.

Jason has been recognized by both *IFLR1000* and *New York Super Lawyers* as a "Rising Star," and he publishes and speaks often about topics of concern to private investment funds. He is the co-author of *Hedge Funds: Formation, Operation and Regulation* (ALM Law Journal Press) and of "Information Security: Obligations and Expectations," a Schulte Roth & Zabel white paper. In his recent speaking engagements, he has discussed co-investments, considerations for managers in their first five years of operations, and marketing opportunities and challenges for funds.

Jason earned his J.D. from Fordham University School of Law and his B.S. from the University of Michigan.

Special Counsel
New York Office
+1 212.756.2433
theodore.keyes@srz.com

Practices

Environmental

Bankruptcy & Creditors' Rights Litigation

Complex Commercial Litigation

Cybersecurity

Insurance

Litigation

Theodore A. Keyes

Ted practices in the areas of insurance law, environmental law and litigation, counseling investment funds and other corporate clients with regard to a wide range of issues and disputes. In addition to environmental and insurance coverage litigation in state and federal court as well as in the context of alternative dispute resolution, Ted's practice includes counseling of clients concerning various specialty insurance policies, including directors' and officers' liability, professional liability and specialty pollution products. He regularly represents investment funds in connection with the negotiation of management liability insurance policies, including working closely with insurance brokers to negotiate favorable policy terms and providing assistance in the event that insurance claims arise. Ted's environmental practice also includes environmental insurance coverage cases, cost recovery actions, regulatory matters and parkland alienation disputes.

Ted has been a co-author of the *New York Law Journal*'s Corporate Insurance Law Column since 2003, and in 2014, he received the Burton Award for Distinguished Legal Writing. His most recent columns include "Insurance Implications of New Justice Department Policy Directive," "Cyber-Risk Insurance Update" and "Return to the Bear Stearns' D&O Insurance Dispute." At recent seminars and events, he has addressed insurance topics of concern to investment funds, including issues related to regulatory risks and examinations, cybersecurity, policy negotiation and understanding key policy terms.

Ted received his J.D. from Fordham University School of Law and his B.A. from The George Washington University.

Partner
New York Office
+1 212.756.2008
robert.kiesel@srz.com

Practices

Intellectual Property, Sourcing & Technology

Cybersecurity

Finance

Vendor Finance

Robert R. Kiesel

Rob chairs Schulte Roth & Zabel's Intellectual Property, Sourcing & Technology Group and is a member of the Finance and Vendor Finance groups. He also co-heads the Cybersecurity Group, which works with 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. Rob focuses his practice on the preparation and negotiation of various types of commercial agreements, including agreements for information technology transactions (outsourcing, software, data and content licensing, hardware supply and strategic alliances), specializing in vendor agreements for investment managers. He also works on agreements for equipment finance and leasing transactions, with an emphasis on vendor finance programs (private label programs, virtual and actual joint ventures and referral programs), and supply agreements for components and finished goods, as well as "take-or-pay" agreements, joint engineering, research & development relationships and technology-sharing arrangements. Rob also handles a broad range of services agreements, including transition and long-term services in merger and acquisition transactions.

Selected by *New York Super Lawyers* as a top business/corporate lawyer, Rob has been a member of the executive committee of the New York State Bar Association's Intellectual Property Section and is a former chair of that section's Committee on the Proposed Uniform Computer Information Transactions Act. He is the author of "Model Cybersecurity Contract Terms and Guidance for Investment Managers to Manage Their Third-Party Vendors" in *The Cybersecurity Law Report,* and he is co-author of "Securities, Futures Regulators Increase Scrutiny, Expectations on Cybersecurity" in *Bloomberg Brief — Financial Regulation* and of "Information Security: Obligations and Expectations," an SRZ white paper. He has addressed topics including information security for private funds, and IP and IT strategies in connection with M&A transactions at recent conferences.

Rob earned his J.D., with honors, from the George Washington University Law School and his B.A., with honors in political science, from the University of Louisville.

Special Counsel
New York Office
+1 212.756.2290
michael.yaeger@srz.com

Practices

Litigation

Cybersecurity

Securities Enforcement

White Collar Defense & Government Investigations

Michael L. Yaeger

Michael focuses his practice on white collar criminal defense and investigations, securities enforcement, internal investigations, accounting fraud, cyber crime and data security matters, as well as related civil litigation. He also leads internal investigation and cyber crime-related representations for financial services companies and provides guidance on drafting written information security plans and incident response plans for investment advisers. He spent six years serving in the U.S. Attorney's Office for the Eastern District of New York, where he investigated and prosecuted cases in the Criminal Division and the Business and Securities Fraud Section involving securities fraud, investment adviser fraud, bank fraud, cyber crime, intellectual property crimes, tax fraud, money laundering, health care fraud, false claims act cases, Federal Food, Drug, and Cosmetic Act violations, and other regulatory offenses. He also served as the co-coordinator for Computer Hacking and Intellectual Property crimes. Michael clerked for the Honorable Samuel A. Alito, Jr. of the U.S. Court of Appeals for the Third Circuit (now a Justice of the U.S. Supreme Court), and the Honorable Milton Pollack of the U.S. District Court for the Southern District of New York.

The Legal 500 United States has recognized Michael as a leading lawyer in his field. A frequent speaker and writer, he most recently co-authored "Securities, Futures Regulators Increase Scrutiny, Expectations on Cybersecurity" in *Bloomberg Brief – Financial Regulation*, "New SEC Cybersecurity Guidance: What It Means for Fund Managers" in *The Hedge Fund Journal* and "Information Security: Obligations and Expectations," a Schulte Roth & Zabel white paper. His speaking topics cover issues including cybersecurity and data protection, the convergence of information and physical security of health care information, cyber readiness for financial institutions and managing information security and IT business architecture for hedge funds. He also presents "Treatises and Complex Litigation" as the annual guest lecturer at a Yale Law School research class.

Michael earned his J.D. from Yale Law School, where he was the John M. Olin Fellow of the Center for Studies in Law, Economics and Public Policy. He earned his B.A., with distinction, from Yale University.

Data Protection and Collection: Cybersecurity, Insurance and Data Scraping

I. Cybersecurity

Information security is not only a good idea — it's 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 measures are, best practices that facilitate compliance can and should be developed and followed now. This outline presents information security issues that private fund managers need to address, from complying with the SEC's and the CFTC's cybersecurity guidance, to handling human resources and insurance concerns.

A. Introduction

1. "Reasonable" Cybersecurity

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.

2. Existing Rules

(a) Investment advisers must maintain data security not only because of contractual obligations (e.g., under contracts between the firm and investors or commercial vendors), fiduciary obligations, or for practical business reasons (e.g., to protect trade secrets), but also because of compliance reasons — namely, the existence of federal and state statutes and regulations that require data security. There are two major types of data security obligations:

(i) The Duty to Protect: provide reasonable security for data, systems and communications

(ii) The Duty to Disclose: disclose breaches to affected parties and regulators, and disclose material risks

(b) Right now, the applicable laws are mostly concerned with protecting the personally identifiable information of human beings (e.g., social security numbers or home addresses) ("PII").

(c) At present, 47 states (and Washington, D.C.; Puerto Rico; Guam; and the Virgin Islands) have laws concerning protection of individuals' PII. These include all states other than Alabama, New Mexico and South Dakota. (The National Conference of State Legislatures provides a list of the relevant laws.)[1]

3. Sector-Specific Laws: The Gramm-Leach-Bliley Act[2]

[1] *See* www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[2] Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 (2006).

(a) The two most significant existing federal regulations for investment advisers and investment companies focus on protecting customers' PII.

(i) Section 30 of Regulation S-P[3]: Requires brokers, dealers, investment companies and registered investment advisers to adopt written policies and procedures designed to protect "customer records and information."[4] The protections are expected to be "administrative, technical, and physical."

(ii) 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."[5]

(b) 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.[6]

(c) 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.[7] Entities not regulated by FINRA should look to FINRA's enforcement cases to understand how regulators may approach these issues.[8]

(d) SEC staff expect registered investment advisers to adopt and maintain written information security policies (each a "WISP").

4. Sector-Specific Laws: The Investment Advisers Act

Poor cybersecurity could potentially create liability under anti-fraud and fiduciary rules of both the Investment Company Act and the Investment Advisers Act, especially given that negligence, and not intentional wrongdoing, may be sufficient to ground liability under the acts.[9]

B. Risk Alerts, Guidance and Enforcement: The Regulators' Sustained Interest in Cybersecurity

1. The 2014 Sweep

(a) In April 2014, the SEC's Office of Compliance Inspections and Examinations ("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 would focus on areas

---

[3] Securities and Exchange Commission, Final Rule: Privacy of Consumer Financial Information (Regulation S-P), 17 C.F.R. Part 248, Subpart A.

[4] 17 C.F.R. § 248.30.

[5] 17 C.F.R. § 248.201(d)(1).

[6] *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; 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; 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.

[7] *See* NASD Rules 3010 and 3012, and FINRA has also brought enforcement cases.

[8] *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/.

[9] *See SEC v. Capital Gains Research Bureau*, 375 U.S. 180 (1963) (holding that a violation of § 206(2) may rest on a finding of simple negligence); *SEC v. Steadman*, 967 F.2d 636, 637 (D.C. Cir. 1992) (noting that a violation of § 206(4) does not require that the defendant acted with scienter).

related to cybersecurity."[10] 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 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."

(b) In other words, the data at issue was 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.

2. 2015 Exams

(a) In January 2015, OCIE announced that cybersecurity compliance and controls would be a focus of its exams in 2015. On Sept. 15, 2015, OCIE issued a Risk Alert providing additional information on its focus. Most important, like the April 2014 Alert, the September 2015 Risk Alert included a "sample list of information that [OCIE] may review" in examinations on cybersecurity matters.[11]

(b) Topics addressed in the alert include:

(i) Governance and risk assessment;

(ii) Access rights and controls (including remote access);

(iii) Data loss prevention;

(iv) Vendor management;

(v) Training; and

(vi) Incident response.

3. IM Division Guidance

(a) The IM Division's April 2015 Guidance Update did not contain many surprises given what OCIE had already announced, but it provided additional detail on what reasonable security measures are by identifying specific techniques to consider in preventing, detecting and responding to cybersecurity threats.[12] (These are described below in the section on "Becoming Compliant: Where to Start").

(b) The Guidance Update also confirmed that mishandling cyber risks can result in violations of the securities laws by investment companies and investment advisers. That is, the document expressly contemplates that liability may result from a failure to "tak[e] appropriate precautions concerning information security."[13] In framing this discussion, the Division states

[10] 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--Appendix---4.15.14.pdf.

[11] Securities and Exchange Commission, OCIE, "OCIE's 2015 Cybersecurity Examination Initiative," Vol. 1V, Issue 8 (Sept. 15, 2015).

[12] Securities and Exchange Commission, Division of Investment Management, IM Guidance Update (April 215), No. 2015-02, "Cybersecurity Guidance" ("Guidance Update").

[13] Guidance Update at 5 n.9.

that "fraudulent activity could result from cyber or data breaches from insiders, such as fund or advisory personnel, and funds and advisers may therefore wish to consider taking appropriate precautions concerning information security," citing as support anti-fraud and fiduciary rules under both the Investment Company Act and the Investment Advisers Act.[14] The Division's statement is especially striking given that some courts have held that negligence is sufficient to ground some claims under these statutes.[15]

4. Enforcement Action: *R.T. Jones*

   (a) R.T. Jones, a St. Louis-based investment adviser, consented on Sept. 22, 2015 to entry of a cease-and-desist order relating to poor cybersecurity and a breach of PII. Notably, the breach occurred before OCIE's 2014 cyber sweep, and Marshall S. Sprung, co-chief of the SEC Enforcement Division's Asset Management Unit, acknowledged that there was "no apparent financial harm to clients."[16] Nevertheless, the SEC pursued the enforcement action and fined R.T. Jones $75,000.

   (b) The order states that "from at least September 2009 through July 2013, R.T. Jones stored sensitive [PII] of clients and others on its third party-hosted web server."[17] The server was attacked in July 2013 by "an unauthorized, unknown intruder, who gained access and copy rights to the data on the server," and as a result "the PII of more than 100,000 individuals, including thousands of R.T. Jones's clients, was rendered vulnerable to theft."[18] "Shortly after the breach incident, R.T. Jones provided notice of the breach to all of the individuals whose PII may have been compromised and offered them free identity monitoring through a third-party provider."[19]

   (c) The order further stated that "the firm failed to adopt any written policies and procedures reasonably designed to safeguard its clients' PII as required by the Safeguards Rule [Regulation S-P]."[20]

   (d) Specifically, the order stated that R.T. Jones's policies and procedures for protecting its clients' information did not include "conducting periodic risk assessments, employing a firewall to protect the web server containing client PII, encrypting client PII stored on that server, or establishing procedures for responding to a cybersecurity incident."[21]

5. The CFTC

   (a) Commodity Futures Trading Commission ("CFTC") Chairman Timothy Massad noted in recent keynote speeches that cybersecurity has become "perhaps the single most important new risk

---

[14] *Id.*

[15] *See SEC v. Capital Gains Research Bureau*, 375 U.S. 180 (1963) (holding that a violation of § 206(2) may rest on a finding of simple negligence); *SEC v. Steadman*, 967 F.2d 636, 637 (D.C. Cir. 1992) (noting that a violation of § 206(4) does not require that the defendant acted with scienter).

[16] Press Release, Securities and Exchange Commission, SEC Charges Investment Adviser with Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach (Sept. 22, 2015), *available at* www.sec.gov/news/pressrelease/2015-202.html.

[17] *In the Matter of R.T. Jones Capital Equities Management, Inc.*, Investment Advisers Act of 1940 Release No. 4204, Admin. Proc. File No. 3-16827 (SEC Sept. 22, 2015) at 2, *available at* www.sec.gov/litigation/admin/2015/ia-4204.pdf.

[18] *Id.*

[19] *Id.* at 3.

[20] *Id.*

[21] *Id.*

to market integrity and financial stability"[22] and that the CFTC was working on a rule proposal related to cybersecurity.[23]

(b) On Aug. 28, 2015, the National Futures Association ("NFA"), the self-regulatory organization for the futures industry, submitted to the CFTC a proposed interpretive notice (the "NFA's Proposal") that would apply to NFA Compliance Rules 2-9, 2-36 and 2-49, which generally require firms to diligently supervise their employees and agents or their businesses.[24] The NFA's Proposal provides cybersecurity guidance and focuses on areas similar to those in OCIE's Risk Alert.

(c) A few weeks later the CFC approved the interpretive notice, which will become effective March 1, 2016. It will apply to futures commissions merchants, commodity trading advisors, commodity pool operators, introducing brokers, retail foreign exchange dealers, swap dealers and major swap participants ("Members").

(d) The interpretive notice sets forth the general requirements that Members should implement for their information systems security programs ("ISSPs"), which include cybersecurity guidance and ongoing testing and training obligations. Requirements include the following:

(i) Members are required to implement a written ISSP program (akin to a WISP), and in doing so are encouraged to consider standards such as ISACA's Control Objectives for Information and Related Technology ("COBIT"), and the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (discussed below).

(ii) Members are required to develop an Incident Response Plan to "provide a framework to manage detected security events or incidents, analyze their potential impact and take appropriate measures to contain and mitigate their threat."

(iii) Each Member is also required to provide training for its employees on information security that is tailored to the risks the Member faces.

(e) CFTC commissioner Sharon Bowen suggested that bigger changes may lie ahead when she described "ideas that I think are worth considering if and when we propose a rule on improving system safeguards." These ideas included: (1) requiring each registrant to designate a chief information security officer; (2) requiring registrants to file annual or quarterly reports on the state of their cybersecurity program; (3) requiring that registrants report any material cybersecurity event to the CFTC promptly (with an example of reports being made "within minutes of a significant breach"); and (4) requiring an independent audit or annual penetration testing for all registrants.[25] While some of these proposals are consistent with current best practices, the reporting of any material event "within minutes" would be a new requirement for fund managers.

[22] Timothy Massad, Chairman, CFTC, Keynote Address Before the Futures Industry Association Boca Conference (March 11, 2015).

[23] Timothy Massad, Chairman, CFTC, Keynote Address Before the Beer Institute Annual Meeting (Sept. 9, 2015).

[24] NFA, National Futures Association: Information Systems Security Programs — Proposed Adoption of the Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs (Aug. 28, 2015) (the "NFA's Proposal").

[25] Sharon Y. Bowen, Commissioner, CFTC, Keynote Address Before ISDA North America Conference (Sept. 17, 2015).

C. The NIST Framework: Why It Matters and What It Is

1. Why the NIST Framework Matters

(a) The SEC's sample questions in the April 2014 and September 2015 Risk Alerts and the NFA's interpretive guidance give hints about what "reasonable security measures" might be by steering firms toward the adoption of a published standard such as the one published by the National Institute of Standards and Technology ("NIST"), discussed below.

(b) Both the April 2014 and September 2015 Risk Alerts expressly state that some of the questions track information outlined in the "Framework for Improving Critical Infrastructure Cybersecurity," released on Feb. 12, 2014 by NIST.[26]

(c) Moreover, one question in the April 2014 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)."

(d) 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."[27] It compiles, and makes reference to, similar past frameworks that other organizations have developed, such as COBIT and ISO 27001.

(e) Further, the SEC has pointed to the Framework in places other than the Risk Alerts. 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."[28]

(f) 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.

2. The Nature of the Framework

(a) 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.

(b) The Framework consists of three parts: the Framework Core, the Framework Profile and the Framework Implementation Tiers.

---

[26] 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.

[27] 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.

[28] 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.

(i) "The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors."[29] 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"[30] and allow an organization to learn from past security incidents.

(ii) "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."[31]

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.

(iii) 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."[32] In determining what Tier they desire, firms should determine which level meets the firm's goals and "is feasible to implement."[33]

D. Becoming Compliant: Where to Start

1. Firm-Level Risk Assessments

(a) 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)."[34]

(b) The SEC is concerned with firms' vulnerability to cybersecurity risks in general, including "misappropriation of funds, securities, … [and] Firm information[.]"[35] Managers should accordingly review existing related policies, such as controls on processing redemption requests and IT safeguards, in a cybersecurity context.

[29] The Framework, at 1.

[30] *Id.* at 4.

[31] *Id.* at 5.

[32] *Id.* at 9.

[33] *Id.*

[34] Risk Alert, Question 24, at 6.

[35] *Id.* at 7.

(c) 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.

(d) Consider doing a gap analysis. Discover where the gaps in the firm's security are and close them.

(i) A gap analysis is an analysis of what you have done, where you are now, and where you want to go.

(1) "What you have done" includes any previous security reviews or audits.

(2) "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.

(3) "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.

(4) 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).

2. Cybersecurity Personnel

Many of OCIE's questions in its Risk Alerts 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. Compliance personnel should be familiar with the division of labor in the technology department.

3. Records of Cybersecurity Incidents

(a) Firms should maintain appropriately detailed records relating to cybersecurity incidents. This is one of the more significant parts of the April 2014 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. To be sure, OCIE is not asking firms to catalogue tech support tickets; it is, however, seeking granular detail on particular security incidents, both retrospectively and going forward. For example, Question 24 of the April 2014 Risk Alert 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 April 2014 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."[36]

(b) 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.

4. 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. A good back-up policy is an essential part of protection against cryptographic extortion malware attacks ("ransomware" attacks) in which the attacker encrypts all of a firm's data and blackmails the firm in exchange for the decryption key.

5. Specific Techniques and Technologies Mentioned by the SEC

(a) As noted above, the IM Division's Guidance Update lists specific techniques that firms should consider in their efforts to "prevent, detect, and respond to cybersecurity threats." These include:

(i) Controlling access to various systems and data via management of user credentials, authentication and authorization methods;

(ii) Data encryption;

(iii) Firewalls;

(iv) Restricting the use of removable storage media (e.g., USB drives);

(v) Deploying software that monitors technology systems for unauthorized intrusions;

(vi) Network segregation; and

(vii) System hardening.

(b) The Guidance Update defines system hardening to mean "removing all non-essential software programs and services, unnecessary usernames and logins," and "ensuring that software is updated continuously."

[36] *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.").

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

1. Human Resources

(a) 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.

(i) 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.

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

(1) Lost or Stolen Devices: Mobile devices are more likely than desktop computers to be lost or stolen.

(2) Cloud-Based Storage: Firm data saved in "cloud" storage by employees may be unsecure and out of the firm's reach.

(3) Wireless (In)security: Data traveling on unsecured wireless networks can easily be stolen.

(4) Downloads/Uploads: Malware may cause damage to a firm's system and threaten its security.

(5) Friends and Family: Mobile devices may be accessed by friends or family.

(b) Disgruntled/Disloyal/Terminated Employees

(i) 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").

(1) ECPA: Title I prohibits wiretapping by private entities 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 parties to the communication are informed that they are 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.[37] Some courts have held, however, that if the communications pass through firm servers or are stored on firm equipment (e.g., hard drives), employers may access personal email and social media posts.[38]

(2) 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.[39]

(3) Twenty-four states (Arkansas, California, Colorado, Connecticut, Delaware, Illinois, Louisiana, Maine, Maryland, Michigan, Missouri, Montana, Nevada, New Hampshire, New Jersey, New Mexico, Oklahoma, Oregon, Rhode Island, Tennessee, Utah, Virginia, Washington and Wisconsin) 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.

(ii) To avoid running afoul of these statutory protections, and to protect firm information, firms should:

(1) Obtain advance authorization to access and wipe the firm's information stored on employee-owned mobile devices;

(2) 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);

(3) Clearly delineate where work cannot be done (e.g., prohibit firm work on personal email accounts); and

(4) Craft policies and procedures 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.

(iii) Proprietary and Trade Secret Information

(1) 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.[40] The evidentiary burden is difficult to meet when the information walks out the door every day in employees' pockets.

---

[37] *See, e.g.*, *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008).

[38] *See, e.g.*, *Front, Inc. v. Khalil*, 2013 N.Y. Misc. LEXIS 3157 (N.Y. Co. 2013).

[39] *See, e.g.*, *Rajaee v. Design Tech Homes, Ltd.,* 2014 U.S. Dist. LEXIS 159180 (S.D. Tex. 2014).

[40] *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).

(2) 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.

(3) To protect firm information, in addition to using traditional measures such as confidentiality agreements and policies, firms should take technical precautions, including 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).

(iv) Employee Speech Protections

(1) 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.

(2) 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.

(3) 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.[41] 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.[42] Policies should, however, prohibit employees from using systems that an employer cannot access (such as personal web-based emails) for business.

(v) 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.

(vi) Elements of a BYOD Policy

(1) Restrictions: A comprehensive BYOD policy should include provisions regarding password protection, encryption of firm data that is stored on the device, lock or

[41] *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).

[42] *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).

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.

(2) 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.

(3) 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.

(4) 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.

(5) 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.[43] 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.

2. Third-Party Risks: Vendor Management

(a) Risks to investment advisers from third parties, and specifically vendors, are a major concern of the SEC. Such third parties include fund administrators, prime brokers, consultants and commercial vendors. Regulators are concerned about the firm's management of third-party vendors, including cybersecurity risk assessment of vendors, training materials used for

[43] OCIE, Investment Adviser Use of Social Media, National Examination Risk Alert (Jan. 4, 2012), at 2; *see* 17 C.F.R. § 275.204-2.

vendors, segregation of sensitive data from third-party access, and security applied to control remote systems access by vendors.

(b) Vendors currently face an array of forms all seeking the same information but using different terms and formats; there is not yet a standard Due Diligence Questionnaire ("DDQ"). Some industry groups are trying to develop a standard, however. For example, the Alternative Investment Technology Executives Club ("AITEC") has designed a document. It is also possible that in the near future, SOC 2 compliance certification will be the industry standard and a lot of DDQs can be avoided with accounting firm certification.

(c) The Diligence Process: Choosing a Vendor

(i) 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.

(ii) 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.

(iii) Ask for and review the vendor's written information security program, business continuity plan, vendor management plan and incident response plan. It is standard practice for the vendor to provide copies of the plans and agree to be contractually bound by the plans.

(iv) The vendor should advise what industry standards it follows (such as ISO or NIST).

(v) The vendor should identify any subcontractors that will have access to sensitive information and should provide diligence material for each subcontractor.

(vi) The vendor should agree to preserve information consistent with any instructions the firm provides, including any litigation and regulatory holds.

(vii) The firm should incorporate data security requirements into its vendor contracts. An 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.[44] These provisions apply to firm-hosted licensed software, vendor-hosted software-as-a-service, and cloud-based vendor arrangements.

3. Practical Recommendations

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

(a) Employee Training: The most important defense against phishing attacks is to train employees not to interact with suspicious emails.

[44] *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/.

(b) Passwords and RSA Security Codes: Restricting system access to users that belong on the system is an obvious and reasonable requirement.

(c) Email Filters: Spam filters are a significant block to phishing attacks and malware.

(d) 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.

(e) Technological Devices: Technological devices such as email sandboxes (which allow email to be checked for malware before it 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.

(f) Limitation on Large Downloads: Restricting flash drive downloads by employees limits information lost through employees.

F. Data Breaches

1. Incident Response Plan

(a) The purpose of an Incident Response Plan is to define a firm's procedures for reporting and responding to security incidents that may compromise the availability, integrity and confidentiality of a firm's information systems, network resources or data.

(i) Of course, as with all plans, the point is to develop a course of action before a problem occurs. This is better than assembling one after the breach happens at 8:00 p.m. on New Year's Eve.

(ii) As ever with compliance documents, terminology varies, but one way to think of the plan is in six parts: Preparation, Identification, Containment, Mitigation, Recovery and Follow-Up.

(1) Preparation: Developing and testing procedures, and training personnel.

(2) Identification: Assigning responsibility for managing the response to an incident, determining the scope of the incident, and, if appropriate, notifying the security incident response team.

(3) Containment: Assessing the risk of continued operations and preventing further loss or damage.

(4) Mitigation: Determining the cause of a security incident and plugging the holes.

(5) Recovery: Returning all data and services impacted by a security incident to full operational status.

(6) Follow-Up: Identifying lessons that make future responses more effective.

(iii) Preparation should include maintaining and analyzing logs on information systems and network resources. All information systems and network resources should use synchronized time so that simultaneous, near-simultaneous, or contiguous events on

different systems can be properly identified. Preparation should also include regular backing up of information systems, and regular restoration tests to ensure the backup media is usable.

(iv) In drawing up a plan, don't just think of the dramatic incidents. 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. And failing to handle the more prosaic events is more embarrassing, and thus potentially more damaging.

(v) Assemble a team that includes various parts of the firm such as:

(1) Tech security;

(2) Tech operations;

(3) PR;

(4) Audit; and

(5) 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.

(6) Develop responses to the most likely attacks (e.g., phishing and insider threats).

(7) Test the response plan — regularly, not just when it is first developed.

(8) 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.

(9) One helpful resource is NIST's Computer Security Incident Handling Guide.[45]

2. Reporting

(a) 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.

(b) 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.

(c) 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 firm lacks sufficient contact information for the affected persons, or if the firm can show that notice will cost more

[45] *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.

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.

(d) 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.

3. Attorney-Client Privilege and Incident Response

(a) Try to protect your deliberations. It will make the substance and outcome of your third-party deliberations better.

(b) Merely copying your lawyer on a communication doesn't make it privileged.

(c) 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.

4. Evidence Collection

(a) Document as much as possible — actions that are performed by IT, conversations with users and system owners regarding the incident, etc.

(i) The point is to know what happened when, and what the decision-making process was.

(1) This information may help a firm to improve its future responses.

(2) 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.

(b) "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."[46]

(c) 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?

5. Communicating and Working with Law Enforcement

(a) Under many state laws, a firm that is cooperating with a criminal investigation may delay its breach disclosure to affected individuals.[47]

(b) Some things to consider:

[46] *Id.*, Appendix G, at 68.

[47] *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).

(i) 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.[48] So getting law enforcement involved usually means diminishing control.

(ii) 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.

(iii) Law enforcement has investigatory tools that private firms do not (e.g., search warrants and contacts in international law enforcement).

(iv) 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.

(v) Get outside counsel involved in dealings with law enforcement.

(c) 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.

(d) What will law enforcement want?

(i) 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.

(ii) Law enforcement may want assistance with undercover operations.

(iii) Preserve Evidence: Don't assume that you should 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.

G. Insurance

The market for cyber risk insurance coverage is growing and more financial services entities, including investment advisers, are considering purchasing coverage to mitigate losses associated with data breaches.

1. Survey Results

(a) OCIE's Cybersecurity Examination Sweep Summary (February 2015) indicates that:

(i) 58 percent of the broker-dealers surveyed maintain insurance for cybersecurity incidents.

(ii) 21 percent of investment advisers have purchased insurance that covered losses and expenses due to cybersecurity incidents.

(b) The *HFMWeek*/JLT Specialty Survey (Fall 2015) indicates that:

[48] *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.).

(i) 15 to 20 percent of hedge funds have purchased cyber risk insurance.

(ii) Of those that have not purchased, 28 percent of hedge funds "want to learn more" about cyber insurance; 19 percent don't know what it is or never heard of it.

2. Traditional Insurance Policies

(a) Crime Policies and Fidelity Bonds

(i) Crime policies may provide coverage for theft of funds or tangible property such as losses due to computer theft, forgery or electronic fraud.

(ii) These policies do not typically provide coverage for loss due to stolen data, unauthorized disclosure of information, or system losses due to a virus or other electronic attack.

(b) General Liability Policies

(i) General liability policies typically provide coverage for damages from bodily injury or property damage caused by an occurrence. This coverage does not typically extend to data breach loss.

(ii) Some general liability policies also provide coverage for personal and advertising liability. In order for such coverage to be triggered, the loss has to arise from publication that violates a person's right to privacy. Courts rejected data breach claims under general liability policies in the *Sony* and *Recall Total Information Management* cases.[49]

(1) In *Sony*, in connection with the Sony PlayStation data breach, the New York court held that the activities of third-party hackers did not constitute "publication" by the policyholder and therefore rejected Sony's claim for coverage.

(2) In *Recall Total Information Management*, the Connecticut Supreme Court affirmed the ruling that the loss of computer tapes containing PII of employees did not trigger the general liability policies because there was no "publication" of the information stored on the tapes.

3. Cyber Risk Insurance Policies

(a) Application and Underwriting

(i) To apply for cyber risk insurance, an investment manager will need to fill out a fairly extensive application that describes, among other things, the type of confidential records maintained, network and computer systems, security controls, and internal information security policies and procedures.

(ii) This information is evaluated by the insurer's underwriting and loss control professionals. This process can provide the investment manager with valuable feedback concerning its information security profile.

(b) Coverage for Third-Party Claims

[49] *Zurich American Insurance v. Sony*, 2014 WL 3253541 (N.Y. County Feb. 24, 2014); *Recall Total Information Management, Inc. v. Federal Insurance Co.*, 317 Conn. 46 (Conn. 2015).

(i) Policies should cover claims by third parties: customers, investors, business partners and regulators.

(ii) Such claims may include, for example, claims for damages arising from unauthorized disclosure of personal and financial data, failure to detect and prevent a data breach, and destruction of critical business records. Third-party claims may also include breach of the insured's own written privacy policy or the violation of applicable privacy laws or regulations. Some policies also provide coverage for third-party claims for libel, slander, defamation, copyright infringement, invasion of privacy, or other claims based on material published on a website or social media space.

(iii) Coverage includes defense costs, which can be significant. For example, news reports of a data breach in the retail arena are often followed soon after by a purported class action lawsuit seeking damages on behalf of customers. These class action lawsuits often face significant obstacles, in particular with regard to standing and damages, but defense costs can still be significant.

(c) Coverage for First-Party Claims

(i) First-party claims include claims for costs incurred to investigate and respond to data breach incidents. Covered costs should include fees for computer experts, legal counsel and crisis management professionals.

(ii) Covered loss may include:

(1) Data restoration costs;

(2) Computer forensics to analyze the scope and cause of a data breach;

(3) Legal analysis of applicable law regarding reporting and notification;

(4) Privacy notification services (including credit monitoring); and

(5) Crisis management expenses.

(iii) Coverage may also include:

(1) Business interruption loss and extra expenses;

(2) Cyber extortion response costs; and

(3) Regulatory fines and penalties.

(d) Exclusions

(i) Cyber risk policies typically contain a lengthy list of exclusions, but many of these exclusions serve the primary purpose of avoiding overlapping coverage by excluding loss that is traditionally covered under other insurance policies including management liability, general liability, employment practices liability and environmental insurance policies.

(ii) Some of the standard exclusions are similar to the exclusions that are contained in D&O and management liability insurance policies. For example, claims arising out of fraud or

intentional illegal conduct will be excluded, as will claims arising out of pre-existing known breaches.

(iii) As cyber claims experience grows, insurers will likely begin to refine exclusions or insert new exclusions unique to cyber issues. The following claims are typically excluded in some form in cyber risk policies:

(1) Claims arising from an act of war;

(2) Claims arising from electrical or mechanical failure that causes an interruption of service from a utility or internet service provider; and

(3) Claims arising from natural disasters.

Some policies may also exclude claims arising from the uploading of music, photos, videos and games.

(e) Comparing Insurance Policies and Carriers

(i) There is currently no such thing as a standard cyber risk policy. Policy forms use similar but different terms and definitions. For example, some forms use the terms "Security Failure" and "Privacy Event," while other forms use the terms "Cyber Liability" or "Network Security Liability" and "Privacy Violation Liability." Over time, we expect the forms to evolve, as management liability policies have, so that the terms are more comparable.

(ii) To compare policies in the current climate, it is important to carefully review defined terms and exclusions to evaluate the scope of coverage. For example, it is important to confirm that loss arising from unauthorized disclosure of an insured's information due to a data breach at a third-party service provider is covered. It is also important to confirm that disclosures arising from the use of mobile devices are not excluded.

(iii) As part of the first-party coverage, many insurers offer a list of preferred vendors that can provide technical, legal and crisis management services in the event of a data breach. In some policies use of the insurers' preferred vendors is mandatory while in other policies it is optional.

(iv) Recently, a few insurers have begun offering some cyber liability coverage as an optional part of their management liability insurance policies. This coverage is likely to be more narrow than what is offered in a separate cyber risk policy.

(v) Premiums for cyber risk insurance for investment managers and funds have remained relatively inexpensive due in part to the absence of noteworthy claims in this market.

II. Data Collection: Web Crawling, Data Scraping and Other Automated Data Collection Methods

A. Many investment managers use automated data collection to analyze prospective investments. Automated data collection uses technological devices called "robots" or "bots" to collect data from

Internet websites. This practice is often referred to as "data scraping,"[50] and the bots are called "web crawlers" or "web spiders."

B. Automated data collection raises legal issues for the data collector, including:

1. Breach of contract (where a website's terms of use[51] prohibit collection);

2. Copyright infringement (where information that is taken by the collector is protected by copyright);

3. Trespass to chattels (where the data collection interferes with the website operator's systems or platform); and

4. Claims under the Computer Fraud and Abuse Act ("CFAA")[52] (where the collection evades technological measures used by the website operator to disable or redirect data-collecting robots).

C. Given these potential issues, investment advisers should consider the following steps:

1. Comply with EULA terms.

Almost every website has an end-user license agreement ("EULA") that a new user is required to click through to acknowledge that the EULA's terms will apply to the user's use of the site. Failure to abide by EULA terms could give rise to a breach of contract claim. Legal issues relevant to assessing a claim include the enforceability of the EULA as a whole (e.g., was the EULA conspicuously displayed and clearly acknowledged by the owner?) and whether the applicable specific EULA terms are enforceable (i.e., are the terms that have been allegedly breached void as unconscionable, illegal or against public policy?). Factual questions include whether the specific use that the data collector is making of the data is prohibited by the language of the EULA and, if so, whether the website operator can show damages. Some EULAs have liquidated damages provisions, which some courts have enforced (when reasonable) in the absence of being able to quantify actual damages.

2. Comply with any robots exclusion protocol.

In addition to the EULA terms, many websites employ a protocol called "robots.txt" that communicates directly with web crawlers and other data collection robots. The protocol provides direction to the robot about which areas of the website may not be scanned or scraped. An investment adviser collecting data should require its bots to follow websites' protocol directions.

3. Do not seek to evade technical measures that a website operator has in place to stop automated data collection.

(a) The Digital Millennium Copyright Act of 1998 ("DMCA")[53] states: "No person shall circumvent a technological measure that effectively controls access to a work protected under this title."

[50] "Web crawling," "web spidering," "web indexing," "Internet indexing," "web scuttling," "web harvesting," "web data extraction" and "data scraping" are all terms that refer to automatic data collection from the web, wherein a robot collector will copy and store data based on the robots set of search parameters. While many of these names are treated as synonyms for each other, generally "web scraping" refers to very targeted data collection (often set to regularly collect specific information from individual websites), while "web crawling" is relatively indiscriminant collection throughout the web (often used by search engines to index hyperlinks from the surface web).

[51] End-User License Agreements or "EULAs."

[52] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2015).

[53] Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 5, 17, 28, and 35 U.S.C.).

The DMCA allows for both civil remedies and criminal penalties for violations under the anti-circumvention provisions. If the violations are determined to be willful and for commercial purposes or private financial gain, the court can order significant fines and/or imprisonment.

(b) Where website owners take steps to prevent automated data collection by a specific party (for example, by blocking the IP address of a bot known to perform automated data collection) and the data collector attempts to evade this restriction (for example, by hiding its IP address), this could give rise to both civil and criminal liability under the federal Computer Fraud and Abuse Act, a statute that prohibits access to a computer, website, server or database either "without authorization" or in a manner that "exceeds authorized access." While the emerging trend is to apply the CFAA only to instances of "hacking," and not to uses of information on publicly available websites that merely violate the EULA, claims may arise under the CFAA in specific instances in which permission to a specific user is revoked and the user nevertheless seeks to continue to access the website.

4. Do not overwhelm the IT systems of the website operator.

   If automated data collection can be shown to take up a measurable amount of the website operator's bandwidth (thus interfering with the website operator's use of its tangible property), this could give rise to a claim of trespass to chattels. Seriously overwhelming a website with multiple or repetitive searches could also be considered to be a denial-of-service attack that may violate the CFAA.

5. Don't compete with the business model of the website being collected from.

   Make sure that the use made of the information being taken is not a substitute for the goods or services offered by the website operator, and that the use does not reduce the revenues of the website operator.

6. Use the collected information internally if possible.

   As a corollary to the "don't compete" rule, if the information is not distributed to investors or published on the data collector's own website, it is less likely that the website operator will consider the use to be competing.

7. To the extent the collected information is made available publicly or to investors:

   (a) Use as little of the website content as possible.

   The more copyrighted material is used, the stronger the website operator's argument is that the data collection has taken the economic value of the material.

   (b) Use factual information rather than more expressive content.

   Merely factual information does not receive copyright protection.

   (c) Do not copy the formatting or presentation of the information from the collected websites.

   In the United States, "thin" copyright protection is given to compilations that contain a modicum of originality in the selection and arrangement of factual information. Copying the formatting or presentation of information from a website gives the website operator the ability to argue that the protectable elements of its website have been infringed.

(d) Attempt to make the use of the website information "transformative."

A use is "transformative" when it alters the original with new expression, meaning or message. Merely copying and reposting website content does not "transform" the collected information and usually does not alter the purpose for which the website operator uses or provides it.

8. Use extra caution when information is collected from non-U.S. websites.

Under U.S. law, databases are not protected simply because they are time consuming and expensive to create, but in some countries databases are protected by copyright. Accordingly, if a given database required a substantial investment to put together, do not take the data on a systematic basis (at least without additional diligence) if the website is operated in a country that allows claims for database right infringement.

9. Think twice about continuing to collect in the face of a cease-and-desist letter.

Continuing to access a website after receipt of a cease-and-desist letter could give rise to a claim under the CFAA. At least one court has held that receipt of a cease-and-desist letter could constitute revocation of authorization such that continued access could give rise to a claim under the CFAA.

10. Consider obtaining a commercial license for the desired service.

Because there is little clarity on the enforceability of EULA terms against data collectors, in cases of doubt investment advisers should consider purchasing commercial licenses to desirable services.

D. Many investment managers do not directly engage in automated data collection, but instead buy data from third-party vendors who engage in the automated data collection. Before entering into such an arrangement, at a minimum, the manager should require the vendor to represent that it has complied with all laws and contractual obligations. In cases where the data and its continued future availability are critical to the manager, the manager may want to perform diligence to ensure that the vendor is in compliance with all the suggested steps listed above (II. C.).

III. The EU Safe Harbor Decision and New Regulations

A. In the late 1990s, both the United States and the EU began to enact data security/privacy legislation to protect the personal information of individuals that is collected and stored electronically by financial institutions.

1. The United States enacted the Gramm-Leach-Bliley Act and Regulation S-P, while the EU enacted the Data Protection Directive.[54]

2. While the United States and EU regulations cover the same topic, the two differ on the treatment of the sharing of individual personal data among affiliates in a corporate group.

(a) In the United States, affiliated groups of companies can share data among each other without getting individual customer approval for such sharing.

[54] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

(b) In the EU, an entity is required to obtain approval from a customer prior to sharing that customer's information with an affiliate or otherwise transferring the data outside the EU.

3. Under the EU Data Protection Directive, any U.S. entity doing business in an EU country through an EU subsidiary would need to obtain customer approval for the EU subsidiary to send EU customer data to its U.S. parent. In cases where a U.S. investment adviser with EU investors runs a global IT back office in New York or Connecticut, it was problematic to process the EU investor data.

B. In 2000, the EU Safe Harbor Decision[55] allowed U.S. institutions to transfer data between EU and U.S. affiliates if the U.S. institution self-certified as to its reasonable data security protections.

C. In October 2015, the EU's highest court determined that the United States is no longer trustworthy with regard to personal data of EU citizens.[56] The court based its decision on revelations by former National Security Agency contractor Edward Snowden regarding U.S. government data surveillance. After the court's decision, U.S. entities were no longer eligible for protection under the EU Safe Harbor Decision. Therefore, for example, an investment adviser with an IT back office in the United States and an affiliate in the EU would have to get approval from individual investors before transmitting and storing the investors' personal nonpublic data to and in its back office. Helpfully, prospective (i.e., advance) approval for affiliate data sharing is effective. Affected investment advisers should therefore review their subscription documents to see if they previously obtained EU investor approval for affiliate data sharing and data exportation.

D. Brand new rules adopted by the EU Parliament in December 2015 require, in this context, investor approval for data exportation to be "distinguish[ed] in their appearance from other matters" and given by the investor "after having been informed of the risks of such transfers."[57] This language seems to require separate (standalone) acknowledgment by EU investors to consent to data exportation. If this is the correct interpretation, a single investor signature on a lengthy subscription agreement would not be effective.

E. It is unclear whether the requirement of separate, distinguished consent will be retroactive so that advisers cannot rely on consent provisions contained in existing subscription documents. U.S. investment advisers with individual EU investors may need to go back and get separate consent from EU investors to export investor data to the United States.

---

[55] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the U.S. Department of Commerce (OJ 2000 L 215, p. 7), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1451331724586&uri=CELEX:32000D0520.

[56] *Maximillian Schrems v. Data Protection Commissioner* [2015] Case C-362/14, ECLI:EU:C:2015, *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=410849.

[57] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, at 45, COM (2012) 11 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

Disclaimer

This information and any presentation accompanying it (the "Content") has been prepared by Schulte Roth & Zabel LLP ("SRZ") for general informational purposes only. It is not intended as and should not be regarded or relied upon as legal advice or opinion, or as a substitute for the advice of counsel. You should not rely on, take any action or fail to take any action based upon the Content.

As between SRZ and you, SRZ at all times owns and retains all right, title and interest in and to the Content. You may only use and copy the Content, or portions of the Content, for your personal, non-commercial use, provided that you place all copyright and any other notices applicable to such Content in a form and place that you believe complies with the requirements of the United States copyright and all other applicable law. Except as granted in the foregoing limited license with respect to the Content, you may not otherwise use, make available or disclose the Content, or portions of the Content, or mention SRZ in connection with the Content, or portions of the Content, in any review, report, public announcement, transmission, presentation, distribution, republication or other similar communication, whether in whole or in part, without the express prior written consent of SRZ in each instance.

This information or your use or reliance upon the Content does not establish a lawyer-client relationship between you and SRZ. If you would like more information or specific advice on matters of interest to you, please contact us directly.

Schulte Roth&Zabel
New York | Washington DC | London
www.srz.com