Demystifying DLP for Investment Advisers

Regulatory Concerns for Data Loss Prevention

E.J. Yerzak, CISA, Vice President of Technology, Compliance Services Consultant, Ascendant Compliance Management, Inc.

The SEC's Focus on Technology

How confident are you in your firm's information technology controls to prevent privacy breaches? The Securities and Exchange Commission is focusing its sights on investment advisers' use of and increasing reliance upon technology – technology which simultaneously improves efficiency and introduces additional complexity to enterprise risk. As the SEC's National Examination Program (NEP) examination priorities for 2013[1] indicate, regulators are keenly interested in the privacy and security issues surrounding the increased reliance upon information technology by investment advisers. Consider that two of the four National Examination Program initiatives identified in the release implicate the role of IT at a firm:

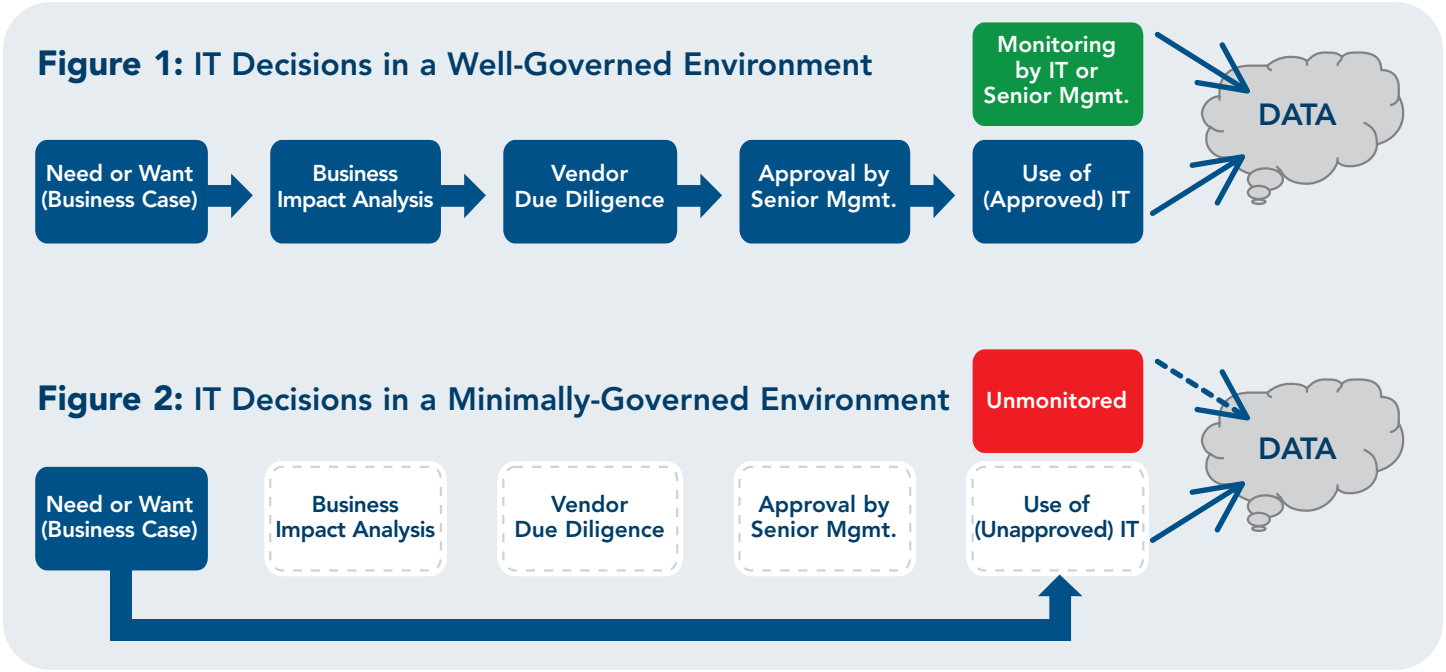
- *Corporate Governance and Enterprise Risk Management*
  Examiners plan to assess how firms "govern and manage financial, legal, compliance, operational, and reputational risks,"[2] with a particular focus on risk and control functions across the firm.
- *Technology*
  Examiners "may conduct examinations on governance and supervision of information technology systems for topics such as operational capability, market access, and information security, including risks of system outages, and data integrity compromises that may adversely affect investor confidence."[3]

The technology focus at advisory firms certainly is not limited to the traditional back-office systems, such as portfolio management, trading, rebalancing, and client/investor web portals. Technology expenditures at investment advisers are predominantly driven by a desire to obtain productivity gains. The ease of use of many cloud-based apps and services, particularly when combined with their ability to be configured and deployed quickly, often incentivizes firm personnel to begin using such cloud-based services to achieve productivity gains prior to subjecting the services to a careful evaluation of the potential privacy and security risks to the firm's compliance program as well as across the enterprise.

Shadow IT: Under the Radar

In a typical, well-governed IT environment, new software and technology services are considered after first determining a business case, performing due diligence on the particular vendor, thoroughly vetting the software or service for alignment with the firm's IT and business needs and risk profiles, and approving the purchase by an appropriate member of senior management. However, as is the case at many investment advisory firms, software can be, and often is, used on an ad-hoc basis by individual employees who have sufficient administrative permissions on their computers to download software. Even without administrative permissions, today's software tends to take the form of a cloud-based application accessed through a web browser and requiring little to minimal installation.

[1] See, "Examination Priorities for 2013," National Exam Program, Office of Compliance Inspections and Examinations, Feb. 21, 2013, SEC Release No. 2013-26.
[2] Id., p. 2.
[3] Id., p. 3.



Employees using unapproved applications are not limited to the technology department or even to the tech-savvy. Rather, these individuals can be anyone at an advisory firm and may include the marketing department, who begin using Dropbox to share sensitive marketing documents with prospective clients or investors. They may include client service representatives, who begin using a Salesforce app on their smartphones to access client information remotely. And they may include a CEO whose desire to use a tablet computer, flash drive, or to forward corporate email to his or her personal email address, resulting in a one-off deviation from established firm policy to appease the CEO.

Technology which is installed by end users with sufficient computer permissions, outside the standard chain of command for IT decisions at a firm, is often called shadow IT or rogue IT[4] due to characteristics of being unsanctioned, unapproved, or otherwise flying under the radar. Unfortunately for many firms, these ad-hoc installations of apps and cloud-based services, when put in place by tech-savvy advisory personnel other than the IT department after careful due diligence, are increasingly subjecting the investment adviser to a Pandora's box of unknown, unmonitored IT and compliance risks.

Investment advisers are required under Rule 204-2 of the Advisers Act of 1940 to maintain books and records relating to their investment advisory business. Rule 204-2(g)(3) further requires that for records which are stored electronically, an investment adviser must establish and maintain procedures

(i) To maintain and preserve the records, so as to reasonably safeguard them from loss, alteration, or destruction;

(ii) To limit access to the records to properly authorized personnel and the Commission (including its examiners and other representatives); and

(iii) To reasonably ensure that any reproduction of a non-electronic original record on electronic storage media is complete, true, and legible when retrieved.[5]

When advisory personnel configure email rules to automatically forward corporate email to personal email addresses, difficulties arise in controlling the flow of proprietary company information and intellectual property outside the firm. The same can be said for investment advisers which permit or otherwise fail to restrict the following activities:

- The use of personal smartphones or communications devices to access corporate email and attachments, without appropriate access controls to safeguard the devices;
- The use of mobile apps to circumvent technology controls on firm computers. For example, a firm may believe that its policy of accessing client data in Salesforce or a similar CRM from encrypted firm computers is adequate, while failing to restrict the use of the mobile Salesforce app to access the same data from an unencrypted smartphone;
- The use of unencrypted USB drives, also known as flash or thumb drives, or unencrypted CDs or DVDs to store or transmit files;
- The sending of personal, non-public information or confidential information through unencrypted email; and
- The use of cloud-based file sharing and file storage services, such as Dropbox, Box, FileShare, and Evernote. Without appropriate procedural and technological controls, these services could enable confidential information from being placed on external machines and accessed or retrieved remotely via computer or smartphone app. Moreover, settings to automatically delete files after a set time period (which are great from a privacy standpoint) may cause headaches for the compliance department attempting to conduct email surveillance or to archive such files for recordkeeping purposes.

The existence of shadow IT is not always a privacy or security problem in and of itself, if end users are diligent enough about complying with the firm's privacy policy and other related policies and procedures. However, shadow IT demonstrates a lack of IT governance and risk management by the firm. In addition, shadow IT overseen by end users can result in software vulnerabilities remaining unfixed long after a patch has been released to address a known security issue (e.g. security bugs in Java, Flash, or Adobe Reader).

[4] See, Julia King, "The Upside of Shadow IT," Computerworld, Apr. 23, 2012, available at http://www.computerworld.com/s/article/9226415/The_Upside_of_Shadow_IT.

[5] 17 C.F.R. 275.204-2(g)(3).

Nonetheless, as regulatory scrutiny of investment advisers' IT controls expands through OCIE's examination priorities and newly adopted rules such as Regulation S-ID, and as the number of violations and sanctions for IT-related breaches of Regulation S-P and other regulations increases, the need for greater control over data loss becomes evident.

Enforcement Actions Highlight Privacy and Data Security Issues

Over the past several years, both the SEC and FINRA have brought enforcement actions and sanctions against investment advisers and broker-dealers for inadequate safeguards over client data. Below is a representative sample of these actions, and the firm names have been redacted.

December 2007: A broker-dealer failed to encrypt an internal database containing sensitive client information. A hacker acquired the data and then held the data for ransom. The firm was fined $375,000, and was required to cover losses and identity theft protection for its clients at a cost of approximately $2.3 million.

July 2008: A firm was sanctioned $125,000 because it did not have strong controls to prevent new employees from bringing in material, nonpublic information when they joined, or from taking such information when they left the firm's employment.

September 2008: A firm was subject to an enforcement action for failing to adopt policies and procedures reasonably designed to safeguard client information, such as maintaining updated security software, firewalls, and antivirus protections. The firm was targeted by several hacking attempts, and the firm's controls were insufficient to prevent clients from identity theft. In announcing this violation, Linda Chatman Thomsen, SEC Director of the Division of Enforcement at the time, stated, "With the increase in the number of incidents involving information security breaches, regulated firms must be vigilant about satisfying their obligation to protect customer information from anticipated threats and unauthorized access."

October 2009: A dually registered investment adviser/broker-dealer was sanctioned $100,000 for failing to protect client data from a hacker, who was able to steal login credentials through a virus on an employee's computer, and for failing to follow procedures once the firm was aware of the data breach.

April 2011: Several employees of a firm were sanctioned for their roles in implementing insufficient controls to properly safeguard client information and for ignoring red flags of data breaches.

May 2013: A firm was sanctioned $7.5 million for not properly configuring its email systems to ensure that emails were archived and subject to surveillance.

While several of the above cases were initiated by FINRA against broker-dealers, others were brought by the SEC. The recently adopted Regulation S-ID (Identify Theft Red Flags Rules) may result in a significant uptick in such cases brought by the SEC. Investment advisers act as fiduciaries for their clients, and it is critically important that advisers protect the client data entrusted to them and over which they have access.

Data Loss Prevention: Plugging the Holes

Data loss at investment advisers is not always intentional. Data loss can also occur as a result of the inadvertent deletion of a file or the unintentional disclosure of confidential information. The process of effectively preventing or mitigating data loss involves three essential steps:

1. Identify the likely methods of data loss and privacy breaches at your firm;
2. Classify your firm's data; and
3. Implement administrative, procedural, and technical controls to address the methods of data loss and breach in a manner commensurate with the sensitivity of the data to be protected.

A. Identify the Likely Methods of Data Loss and Privacy Breaches

The first step for investment advisers seeking to limit data loss is to assess all of the channels through which information may depart the firm. Data loss may occur through any of the following, for example:

- Email
- Cloud-based applications
- Traditional software left unpatched
- USB/flash/thumb drives
- Unencrypted laptops
- Mobile devices, including smartphones and tablets with access to firm information

Firms may wish to consider brainstorming sessions to think creatively for possible data breach methods. In addition, it is recommended that firms consult online sources of data breach information, such as www.privacyrights.org/data-breach.

Finally, consider the potential underlying motives for rogue employees at your firm to contribute to data loss and privacy breaches. Is there an employee who was recently disciplined by your firm? Are you aware of an employee considering a departure to another investment adviser, and who may decide to send your firm's client list to his or her new firm by uploading it to Dropbox for later retrieval?

B. Classify Your Firm's Data

Investment advisers should know not only what IT assets they own and what machines and devices are accessing their computer networks, but also the nature of the data stored on those networks and systems. Controls to protect data from data loss may vary with the sensitivity of the underlying data to be protected. For example, it would be advisable to have strong controls in place to detect if an employee attempts to email a client list outside the firm, whereas an outright ban on sending attachments externally would seem overkill if the attachment is merely a grocery list being sent by an employee to a spouse or partner.

Data owners (i.e. the creators of documents) are generally in the best position to identify the classification level of the document. Typical classification schemes use categories such as high/medium/low sensitivity, or confidential/sensitive/public.

C. Implement Appropriate DLP Controls

Once your firm has identified its IT assets and categorized its documents according to a confidentiality hierarchy, the final step is to implement appropriate data loss prevention ("DLP") controls to prevent or mitigate data loss and privacy breaches. Controls may be procedural in nature (e.g. a firm policy prohibiting the use of Dropbox or Evernote for any purpose, or a policy permitting limited use of such services by approved personnel only). Procedural controls will necessitate changes to your firm's compliance or operations manual. However, in the absence of accompanying technological changes, it can be difficult to effectively monitor or enforce your firm's DLP and privacy protections.

Technological DLP controls range from the simple (disabling all USB ports on firm computers, which may be counterproductive) to the complex (continuous port-scanning for the use of unapproved file-sharing services on the firm network, and automatic quarantine and notification to the CCO for outgoing email attachments flagged as containing confidential information).

DLP solutions should work in tandem with your policies and procedures, and to the extent feasible, with your existing email and messaging systems. A sample list of DLP controls is provided below.

- Capability to manually encrypt an outgoing email
- Automatic, rules-based email encryption which detects patterns of potential confidential or private information, such as account numbers, social security numbers, etc.
- Centralized patch management for software applications used by the firm
- URL-based filtering and restriction of web-based applications
- Port-based filtering and restriction of network applications
- Intrusion detection system (IDS) or intrusion prevention system (IPS) to handle external attempts to obtain your firm's data
- Whitelisting or blacklisting apps
- Allowing third-party apps such as Dropbox, Box, and Evernote, but by approved personnel only, and for specifically defined purposes or limited to specific data
- Mobile device management (MDM) software
- Implementing other third-party hardware or software DLP controls to monitor for sensitive data traversing your firm's network. Some DLP vendors provide tools which can provide reporting capabilities to senior management on the number of incidents prevented and the types of data breaches halted.

After flagging a potential data loss occurrence from your organization, what responsive action will your firm consider taking?

- Do you prefer to quarantine the content and prevent the message, email, data, or attachment from being sent?
- Do you want to alert the user who attempted to send the data outside your firm?
- Would you prefer to notify the employee's supervisor?
- Will the supervisor be able to review the flagged data loss event and click a button to confirm that the data is permitted to be sent outside the firm?
- If a message containing sensitive data was about to be sent unencrypted and your DLP system stops the email at your network perimeter before it is sent, do you want to apply automatic encryption and allow the message to proceed in an encrypted format?

Data Lost = Reputation Lost

The examples stated above are just some of the concerns raised which data loss prevention controls can help address. Understandably, there is no specific rule under the Advisers Act of 1940 which provides that investment advisers must have data loss prevention controls in place to safeguard against data loss and privacy breaches. But as evidenced by the number of enforcement actions referencing data security issues, the number of new regulations with a technology focus (e.g., Regulation S-ID, Regulation SCI), and the SEC's published examination priorities list, good compliance is about more than just following the black letter rules because it makes good business sense. It is about protecting the data of your clients. It is about helping your firm to lower its level of enterprise risk. Increasingly, many of those risks are related to your firm's use of technology.

Hyperbole aside, it is a reasonable assumption that nearly every registered investment adviser is one significant data loss or privacy breach away from going out of business. A firm's reputation means everything to clients. Having to disclose that your firm's lack of IT controls exposed or compromised your clients' data and personal information, or being subjected to a hefty regulatory fine for lax oversight of your IT systems, can spell the endgame for many advisers.

E.J. conducts on-site compliance program reviews, risk assessments, due diligence reviews, trade blotter analysis, and consults on a variety of other matters for Ascendant's clients, including advisers to private funds and funds of funds. E.J. produces the ComplianceCasts™ Minute podcast series available on Ascendant's website, and has authored articles and alerts on emerging regulatory and technology issues. As a Certified Information Systems Auditor (CISA®) and Certified in Risk and Information Systems Control (CRISC™), he is Vice President of the technology team at Ascendant which performs IT risk assessments of firms' technology controls. E.J. brings experience in both information technology and law to the compliance arena. Prior to Ascendant, E.J. served as a federal law clerk to the Chief United States Bankruptcy Judge for the District of Connecticut, and worked for 8 years as a Partner and Senior Consultant at a New York-based firm, where he managed several software development teams, drafted manuals and specifications, and provided web-based demonstrations.
E.J. holds a Bachelor of Arts in both English and Computer Science, Magna Cum Laude, from Colgate University, a Master of Science degree in Computer Information Technology from Central Connecticut State University, as well as a J.D., Magna Cum Laude, from Quinnipiac University School of Law. He is licensed to practice at the State Bar of Connecticut and in federal court before the U.S. District Court for the District of Connecticut.