The Metropolitan
Corporate Counsel®
National Edition
www.metrocorpcounsel.com
Volume 22, No. 4 April 2014

Cybersecurity Update: SEC Announces Scrutiny For Investment Companies And Investment Advisers

Kenneth L. Greenberg

STRADLEY RONON STEVENS & YOUNG, LLP

The Securities and Exchange Commission (SEC) has announced that cybersecurity will be an area of regulatory focus during 2014. The National Exam Program (NEP) run by the SEC's Office of Compliance Inspections and Examinations (OCIE) has included "information security" as an examination priority for 2014 for each of NEP's four program areas:

1. investment companies and investment advisers;
2. broker-dealers;
3. exchanges and self-regulatory organizations; and
4. clearing and transfer agents.[1]

Among items that may be reviewed by the SEC inspection staff during an inspection of an investment company or its investment adviser are the policies and procedures designed to address computer security, identity theft (red flags), privacy and business continuity. Investment advisers and their investment companies will also be expected to have reviewed the computer security policies of their third-party service providers.[2] In addition, the SEC announced that it will host a roundtable at its Washington, DC headquarters on March 26 to discuss "cybersecurity and the issues and challenges it raises for market participants and public companies and how they are addressing those concerns."[3]

Kenneth L. Greenberg

Overview Of Current Computer Crime And Its Costs

Stories about computer data breaches, such as the *Adobe* (2.9 million customers affected), *Target* (70 million customers affected) and *JPMorgan Chase & Co.* (456,000 customers affected) incidents, have figured prominently in the news.[4] While recent national media attention has focused on a few large-scale, high-profile data security breaches like those that affected national retailers *Target* and *Neiman Marcus,* data security breaches are widespread and continue to grow in number and scale. For 2013, the Identity Theft Resource Center (ITRC) reported 614 data breaches involving 91.9 million compromised records, which represented a 30 percent increase over the 2012 data security breaches tracked by the ITRC.[5] Similarly, a global study on data breach investigations published by the Verizon RISK Team reported that in 2012 there were 47,000-plus reported security incidents, of which 621 involved confirmed data disclosures that compromised at least 44 million records. Financial organizations were involved in 37 percent of these 2012 data security breaches.[6]

The stakes for businesses that experience a data security breach are high and entail significant financial consequences. The Ponemon Institute's "2013 Cost of Data Breach Study: Global Analysis" reports that, on average, a data breach costs U.S. companies $5.4 million per data breach, or $188 per compromised record (average number of compromised records: 28,765). Ponemon further analyzed the $5.4 million in costs and divided the components of that cost as follows:

- $3,030,814 **Lost business costs** (e.g., reputation losses, diminished goodwill, increased customer acquisition activities and/or abnormal customer turnover).
- $1,412,548 **Post-data breach costs** (e.g., special investigative and remediation activities, legal expenditures, provision of identity theft protection services, and/or increased help desk activities).
- $565,020 **Customer notification costs** (e.g., creation of contact databases, determination of legal notification requirements and postage).
- $395,262 **Detection and escalation costs** (e.g., forensic and investigative activities, audit service and crisis team management).

Current Regulations Impacting Cybersecurity

In light of the regulatory focus on cybersecurity, legal and compliance personnel at investment advisers and investment companies should be familiar with the relevant regulations of the SEC and the states that address cybersecurity.

Federal Privacy Regulations. Enforcement actions initiated by the SEC relating to computer security are often grounded in violations of Regulation S-P.[7] Rule 30 of Regulation S-P, which implemented the privacy provisions in Title V of the Gramm-Leach-Bliley Act of 1999 (the G-L-B Act),[8] requires the following:

Every broker, dealer and investment company, and every investment adviser registered with the Commission, must adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. These written policies and procedures must be reasonably designed to:

1. insure the security and confidentiality of customer records and information;

***Kenneth L. Greenberg** is a Partner in Stradley Ronon's Philadelphia, PA office. He counsels investment companies, investment advisers and broker-dealers on regulatory matters relating to separate accounts and pooled investment products, including registered and unregistered and open- and closed-end investment companies. For the footnotes to this article, please visit http://www.metrocorpcounsel.com/articles/27832/cybersecurity-update-sec-announces-scrutiny-investment-companies-and-investment-advis.*

Please email the author at kgreenberg@stradley.com with questions about this article.

2. protect against any anticipated threats or hazards to the security or integrity of customer records and information; and

3. protect against any unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

The enforcement actions highlight several broad categories of misconduct involving Regulation S-P, including inadequate policies and procedures,[9] failure to follow up on discovered cybersecurity issues,[10] and employee misconduct.[11]

Federal Identity Theft Red Flags Regulations. Regulation S-ID[12] requires financial institutions (including investment companies and their advisers) that offer one or more covered accounts (including any account maintained by a mutual fund or its agent that permits wire transfers or other payments to third parties) to develop and provide for the continued administration of a written program to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

Business Continuity. The SEC has not adopted a specific regulation that requires the use of a business continuity plan. However, in the adopting release for Rule 38a-1, which addresses compliance programs for investment companies and investment advisers and mandates the adoption and implementation of written policies and procedures designed to prevent the violation of the Federal Securities Law,[13] the SEC declared that it expected that an investment adviser's compliance policies and procedures, at a minimum, should include a business continuity plan and expressed its belief that:

> an adviser's fiduciary obligation to its clients includes the obligation to take steps to protect the clients' interests from being placed at risk as a result of the adviser's inability to provide advisory services after, for example, a natural disaster or, in the case of some smaller firms, the death of the owner or key personnel. The clients of an adviser that is engaged in the active management of their assets would ordinarily be placed at risk if the adviser ceased operations.[14]

State Data Security Breach/Notification Laws. Unlike the federal securities laws for which the National Securities Markets Improvement Act of 1996[15] pre-empted most areas of state securities law other than the anti-fraud provisions, the G-L-B Act, which is the basis of the federal privacy regulations, preserves state authority to address privacy issues and further permits a state statute or regulation to provide greater protections than the G-L-B Act. As of the date of this article, 46 states, the District of Columbia, Puerto Rico, the Virgin Islands and Guam have enacted legislation requiring companies to notify individuals in a timely fashion of data security breaches involving personal information.[16] The notification laws generally require that such notification be "in the most expedient time possible without unreasonable delay consistent with the legitimate needs of law enforcement" (although some states have enacted specific timing requirements).[17] Only Alabama, Kentucky, New Mexico and South Dakota have not adopted a data breach notification law. In addition, Arkansas, California, Connecticut, Indiana, Maryland, Massachusetts, Nevada, Oregon, Rhode Island and Utah have adopted data security laws that require companies to protect state residents' personal information from data breaches and identity theft.[18]

What Can My Company Do To Prepare For The SEC's Focus On Cybersecurity?

In light of the SEC's renewed focus on cybersecurity, below is a list of actions your company should consider taking before the SEC arrives for an inspection.

Review and reassess your data privacy and computer security policies and procedures.

- Are your company's actual practices consistent with the policies and procedures? Do changes need to be made so that policies and procedures better reflect company practices, or do company practices need to change to better reflect policies and procedures?
- Are your policies and procedures staying up to date with technological advances (e.g., do they address the plethora of mobile devices that are now available to employees)?
- Reconsider potential threats to the computer system and the defenses to protect against those threats. Do the defenses adequately address threats? Are firewalls, anti-spam and anti-virus software updated regularly? Are patches for the operating system and other software updated regularly? Does your company have someone responsible for monitoring events to make sure computer system defenses remain responsive to potential threats?
- Does the company understand what information, if stolen, would be the most damaging to its business or its customers, and is that information adequately protected?

Review and reassess the data privacy and computer security policies and procedures of your third-party service providers. While the level of detail of review that you apply to a third-party service organization may not be as exacting as it is for your own organization, do you have a high level of confidence that their data privacy and computer security policies and procedures are sufficient for protecting your company's and your customers' information?

Review and reassess service contracts with third-party service providers to ensure that privacy and computer security issues are adequately addressed. Consider whether an amendment to a service contract may be necessary.

Review and reassess insurance policies. Confirm whether your company's insurance coverage includes losses, remediation costs and litigation costs associated with a data breach, and consider whether such coverage is adequate. Such insurance coverage is evolving, so consider consulting with an insurance broker knowledgeable about the latest policies in the marketplace for the coverage you may need.

Review and reassess your data breach policy.

- Is it sufficiently detailed to provide guidance for what needs to be done immediately in the event of a security breach?
- Does your company have a team already established that can begin to deal with a data breach as soon as it is discovered? Are the various constituencies of your company represented on the team (e.g., management, information security, information technology technical experts, legal, public affairs, business continuity, human resources and facilities management)?
- Is the leader of the team granted sufficient authority so that decisions made by the team may be quickly executed?
- Do you conduct periodic "fire drills" to test the readiness of your company's data breach policy?

Review and reassess record/data retention policies and destroy unneeded data if permitted by books and records requirements of applicable statutes and regulations. In order to limit the universe of information that is susceptible to a data breach, consider whether older or unneeded data must continue to be retained. If a computer or other equipment that holds data on a hard drive is being replaced, make sure that such data is completely erased.[19] In reality, the only way to absolutely guarantee that information on a hard drive is unretrievable may be to destroy the hard drive (which may not be practicable).

Review and reassess your employee education/training programs. Have you conducted training to make employees aware of the various computer threats so they can be recognized when they occur? Does your company require employees to practice computer security best practices (e.g., use passwords with a mix of uppercase and lowercase letters, numbers, and symbols)?

Review and reassess your company's business continuity and disaster recovery plans. Does your company's business continuity plan cover a cyber attack or other type of computer disruption in addition to more commonly covered business disruptions, such as natural disasters and fire?

Test and retest computer networks and systems.