GT GreenbergTraurig

Advisory | Cybersecurity, Privacy & Crisis Management

August 2018

The SEC, Cybersecurity, and Registered Investment Advisers: All in the Same Boat Fighting Cybercrime

Why Ignoring OCIE On Cybersecurity Could Lead to Catastrophe

The Office of Compliance Inspections and Examinations (OCIE) of the U.S. Securities and Exchange Commission (SEC) has recently started to examine the capabilities of domestic organizations to fend off attempted cyberattacks and respond quickly to successful ones to ensure the confidence of investors, limited partners, and public markets in general. Since these attacks can be devastating,[1] OCIE has created guidelines for companies and firms intended to help prevent cyberattacks and minimize risk. Failure to follow these guidelines will likely result in OCIE issuing critical inspection reports or even making referrals to enforcement offices. To guard against disastrous cyberattacks, minimize both organizational and reputational risk, and prevent OCIE or enforcement penalties, companies and firms should understand and implement these guidelines at their earliest opportunity. This benefits both the organization (to avoid potential regulatory fines and penalties, and liability to other parties affected by a breach) and any investors and limited partners, who could potentially lose millions should there be a successful breach.

[1] *See* "The biggest hacks and data breaches of 2018 (so far)," available at https://www.wired.co.uk/article/hacks-data-breaches-in-2018.

Introduction

OCIE is the arm of the SEC that goes out to registered entities to evaluate many aspects of operations and regulatory compliance. The SEC has charged OCIE with the task of evaluating the readiness of regulated investment advisory firms in relation to cybersecurity.[2] In addition to entities such as registered investment companies, registered advisers, broker-dealers, and transfer agents, these firms also include alternative investment and hedge funds, wealth management firms, and private equity funds. The SEC's National Exam Program (NEP), run by OCIE, aims to protect investors, maintain market integrity, and promote responsible capital formation using risk-focused strategies. These strategies, if implemented properly, should improve compliance, prevent fraud, monitor risk, and inform policy.[3] On July 21, 2010, the passing of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) granted OCIE additional authority over more people and entities.

For many years, OCIE has issued an annual exam letter detailing priorities for examinations it will conduct during the year. Since 2010, OCIE has made computer security issues an important item on its list of topics. OCIE has been working with organizations to help them self-assess their ability to mitigate risk and defend against cyberattacks, and to improve their practices in these areas. In 2011, referrals from NEP in cooperation with the SEC's Division of Enforcement resulted in a significant number of enforcement actions. These cases reportedly stopped Ponzi schemes, identified material disclosure omissions and misinterpretations, and illuminated hidden fees/undisclosed remuneration and expenses charged to investors.[4] The SEC uses the data collected from NEP to recognize and monitor risk, brief rule-making initiatives, pursue misconduct, and improve industry practices guided by NEP's general principles: to be data-driven, risk-based, and transparent; to have maximum efficiency with its resources; and to embrace new technology.[5] More recently, OCIE referrals have led to enforcement actions related to poor cyber-security, and to actions derived from actual breaches that have harmed companies or investors.

National Exam Program Risk Alert, 2015:

In April 2014, OCIE published its first comprehensive Risk Alert addressing how SEC-led examinations would help to identify cybersecurity risks and determine the degree of cybersecurity preparedness in the securities industry. In February 2015, OCIE published its conclusions from these observations. This publication deliberated upon legal, regulatory, and compliance issues relating to cybersecurity. After examining 57 broker-dealers and 49 investment advisors, OCIE came to these general conclusions:[6]

1. 93 percent of broker-dealers and 83 percent of investment advisors examined adopted written security procedures and policies, and a large group of the firms operated regular audits to determine compliance with procedures and policies.

2. Many firms used external standards and other outside resources to guide their information security processes and architecture.

[2] SEC OCIE Cybersecurity Initiative and Exam, Secureworks.com
[3] Ibid.; Office of Compliance Inspections and Examinations, SEC.gov/ocie
[4] Examinations by The Securities and Exchange Commission's Office of Compliance Inspections and Examinations, February 2012
[5] Office of Compliance Inspections and Examinations; 2018 National Exam Program Examination Priorities, SEC.gov
[6] Mark C. Amorosi, Marguerite W. Laurent, K. Susan Grafton, András P. Teleki, "A Few Takeaways from the OCIE Cybersecurity Examination Sweep Summary," klgates.com

3. Most of the examined firms engaged in regular risk assessments to find cybersecurity threats, vulnerabilities, and business consequences.

4. Most firms examined conducted inventorying, cataloguing, and/or mapping of their technological resources.

5. Almost 75 percent of the examined broker-dealers, but less than 25 percent of the investment advisors, implemented mandatory actions regarding cyber risk into their contracts with partners and vendors.

6. Almost all firms used encryption.

7. Many firms provided clients with advice to protect information, but more broker-dealer firms did so than investment advisors.

8. More than half of the broker-dealers had cybersecurity insurance, but very few investment advisory firms had it.

9. The clear majority of firms had experienced a cyber incident.[7]

These results show that cybersecurity and risk management improved in these firms, but further improvement is needed to prepare for and defend against cyber incidents. Furthermore, it was shown that broker-dealers generally have cybersecurity practices that are much better suited to the modern world, which is riddled with cyber-risk, than those of investment advisor firms. In response to these 2014 findings, OCIE continued to emphasize cybersecurity compliance and controls in its 2015 Examination Priorities.[8]

The Continuing Examination Process

OCIE devised its Cybersecurity Examination Initiative to further develop its examination practices in response to ongoing security breaches and threats, and to determine the level of cybersecurity preparedness within the securities industry. This includes firms' ability to safeguard broker-dealer customer and investment advisor client information. Public reports have found cybersecurity breaches concerning vulnerabilities in rudimentary controls often went unattended or were simply ignored. As a result, OCIE suggested that examiners collect data on cybersecurity-related controls in addition to examining the implementation of specific firm controls. To encourage improved compliance practices and to improve the SEC's comprehension of cybersecurity preparedness, the SEC release noted that its cybersecurity initiative will emphasize the following areas: governance and risk assessment, access rights and controls, data loss and prevention, vendor management, and incident response.[9] Below is additional information about each of the areas under consideration by the SEC:

Governance and Risk Assessment

The SEC emphasized that examiners should consider whether registrants possess cybersecurity governance and risk assessment processes in relation to the topics discussed. This could reveal whether firms are regularly examining cybersecurity risks and whether controls and risk assessment processes fit

[7] Ibid.
[8] National Exam Program Risk Alert Volume IV, Issue 8, OCIE's 2015 Cybersecurity Examination Initiative, SEC.gov/files
[9] Ibid.

the business needs of the firm. The SEC further suggested that the degree of communication to and participation of senior management (as well as the board of directors) should be thoroughly reviewed.[10] Communication is crucial because the board of directors, management companies, and senior managing directors often hold immense power to effect change within the organization. If they are not informed and updated on the proper cybersecurity protocols, the lack of proper cybersecurity oversight could potentially inflict considerable damage on the organization if there is a breach. Also, adequate communication enables the proper personnel to address the incident as swiftly as possible. The difference between a minor setback and a major disaster in the cybersecurity world could be a matter of mere hours, so continuous communication is a necessity.

Access Rights and Controls

Firms leave themselves especially vulnerable to data breaches if they fail to establish basic controls designed to prevent unauthorized access to private systems and data. Some examples of these important controls are multifactor authentication and updating access rights based on personnel/system changes (meaning authorized current users are given just enough access to do their jobs, but no more). It is important for examiners to review how firms control access to various systems and data through management of user authentication, credentials, and authorization methods. This may include reviewing controls in relation to remote access, consumer logins, and firm protocol when addressing consumer login issues, passwords/passphrases, network segmentation, and tiered access.[11]

Recognizing that many recent cyber invasions to capture data or extort system operators have exploited human weaknesses that allowed access to systems, recent OCIE examinations have shown increased attention to the training provided to organization personnel. As discussed below, training to prevent successful "phishing" attacks and insertion of "malware" into systems is receiving enhanced attention.

Data Loss Prevention

Data breaches can occur due to a lack of strong controls in patch management and system configuration. To minimize data loss, the SEC suggested that examiners assess the method in which firms supervise the volume of content transferred outside the firm by its employees or through third parties. This content includes email attachments and uploads, among other things. It is also important for examiners to assess the methods by which firms watch for unauthorized data transfers and to review how firms authenticate consumer requests to transfer funds.[12]

Vendor Management

Among the largest data breaches (prior to OCIE's NEC Risk Alert Volume IV, Issue 8) were those that resulted from the hacking of third-party vendor platforms, the greatest threat to firms in 2015 according to Booz Allen Hamilton. Despite this threat, PwC found through its 2015 U.S. "State of Cybercrime Survey" that 23 percent of firms did not examine third-party vendors, 19 percent of CIOs had no concern for supply-chain risks, more than half of respondents surveyed did not consider supplier risks at all, and most companies did not create a process for determining the security capabilities of third-party vendors before associating with them.[13] Of course, allowing trusted third parties to have access to the firm's network may create real efficiencies for all parties involved, but OCIE recognized that such access could create a "back door" entry into the firm's network using compromised credentials. Recent examinations of

[10] Ibid.
[11] Ibid.
[12] Ibid.
[13] "Third-Party Security Breaches Sign of Growing Vendor Risk Problem," securityscorecard.com

registered entities are now asking registrants what they do to inspect or otherwise evaluate the controls in place at vendors who are granted access to the organization's systems, and vendors hired to operate systems, provide software, or host data for the registrant. Some of these providers, in order to enhance their own security, are reluctant to share such information with registrant-customers, but OCIE is not always satisfied with that response from the registrant.

Training

Firm employees and vendors can benefit greatly from appropriate training on how to mitigate data risk. Data breaches can result from unintentional employee actions, such as misplacing or losing a device (e.g., a laptop, phone, tablet, etc.), viewing confidential or classified information while connected to an unsecured internet source, or opening messages/downloading attachments/clicking on links from an unknown source. To protect against these potential data breaches, well-trained employees will have location services turned on for all their devices, possess the ability to wipe the data remotely, and confirm the connection is secure (e.g., through a VPN) before viewing confidential/classified information. Finally, through regular employee training and awareness, employees should be equipped to spot suspicious downloads, attachments, links, etc. from unknown sources, and verify that they are safe before opening them. Likewise, good employee training and awareness will help employees understand the potential dangers associated with social media browsing and "watering hole" attacks.

Incident Responses and Business Continuity

In general, firms recognize the growing risk of cybersecurity threats and breaches. Management should be aware that OCIE will want to determine if firms have established policies, assigned roles, evaluated and addressed system vulnerabilities, and created plans to combat and respond to future incidents, as well as to recover from them quickly. OCIE and the SEC are now using extremely complicated data analytics to select exam targets, to focus the scope of examinations and to achieve the most efficient use of SEC resources. Organizations can use similar analyses to help decide which firm data, assets, and services (i.e., "the crown jewels") should be assigned the most security to stop attacks from inflicting severe damage.[14] Business continuity plans allow the firm to prioritize critical systems and get them up and running as soon as possible.

2018 NEP Examination Priorities

OCIE has published five priorities regarding the focus of the NEP for 2018. These priorities follow (in no specific order):

1. Matters of importance to retail investors, seniors, and people saving for retirement
2. Compliance and risks in critical market infrastructure
3. Financial Industry Regulatory Authority (FINRA) and Municipal Securities Rulemaking Board (MSRB)
4. Cybersecurity
5. Anti-money laundering programs

[14] Ibid.

It is prudent for individuals, companies, and firms to emphasize strengthening compliance infrastructure, especially in areas of OCIE focus. Though compliance with OCIE's cybersecurity initiatives cannot successfully ward off all breaches, adherence to the SEC's cyber suggestions could make firms more resilient, and hopefully more secure. Efforts that match industry best practices will help minimize the risk that the SEC will pursue more severe sanctions in the event of an unpreventable breach.

OCIE's Continuing Focus Relating to Cybersecurity

OCIE examinations relating to cybersecurity will continue to include risk assessments, governance, vendor management, data loss prevention, access rights and control, incident response, and training. Due to this prioritization of cybersecurity, the SEC has fined organizations for ignoring responsibilities in cybersecurity procedures and policies. A common fine levied by the SEC is for the violation of Rule 30(a) of Regulation S-P, otherwise known as "The Safeguard Rule." This rule mandates that investment companies, investment advisors, and registered broker-dealers adopt written policies and procedures that facilitate the protection of customer data. OCIE also stated that an organization can still be charged with cybersecurity-related infringements even if the client does not experience financial loss. For example, the SEC fined R.T. Jones Capital Equities Management $75,000 for its lack of cybersecurity procedures and policies relating to a breach of a third party's web server.[15] These fines are arguably nominal compared to the disaster that results from data breaches. Apart from the damage done to consumers, firms often must pay costly legal fees and payouts resulting from consumer lawsuits, repair their damaged reputations, and upgrade their security while investigating the breach (the latter two also being very expensive).[16]

Conclusion

While following OCIE's guidelines effectively does require time and money, doing so can not only spare companies from incurring fees if the guidelines are neglected but also help mitigate cyber risk, prevent cyberattacks, and control the damage resulting from a successful attack. If a successful cyberattack goes unaddressed, the ensuing legal fees, payouts to victims, etc. may damage an organization severely, possibly to the point of no recovery. In other words, spending some resources on cybersecurity and risk management now may significantly lower the risk of losing everything later.

Author

This GT Advisory was prepared by **Paul Ferrillo**. Questions about this information can be directed to:

- Paul Ferrillo | +1 212.801.6598 | ferrillop@gtlaw.com
- Or your Greenberg Traurig attorney

*Special thanks to Louis Faiella IV[¥] for his assistance with this GT Advisory.

[¥] *Not admitted to the practice of law.*

[15] Geeta Malhotra, Matthew J. Saldaña, and Colleen Theresa Brown, "Cybersecurity Identified as an SEC OCIE Examination Priority for 2018," datamatters.sidley.com
[16] Third-Party Security Breaches Sign of Growing Vendor Risk Problem, securityscorecard.com

Orlando. Philadelphia. Phoenix. Sacramento. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.^ Tokyo.¤ Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.