GT GreenbergTraurig

Alert | Financial Regulatory & Compliance/ Data, Privacy & Cybersecurity

May 2019

Summer Is Coming – Are You Prepared for the SEC OCIE Cybersecurity Sweep?

In March 2019 the SEC Office of Compliance, Inspections and Examinations (OCIE) announced it would soon commence its annual "Cybersecurity Sweep" (Cyber Sweep) of registered investment advisers and broker-dealers. If these entities were not already focused on cybersecurity, OCIE's announcement should assure registrants that cybersecurity is not a single frame of a movie, but a feature film with heroes and villains, daily plot twists (like malware) and turns (like spear-phishing). The reality of daily breaches/hacks combined with the watchful eye of the SEC and other regulatory and enforcement bodies should also re-energize registrants to dedicate resources to protect their customers from cyber threats.

The SEC has given us some ideas as to the areas of emphasis for the Cyber Sweep in its 2019 "Examination Priorities" document. OCIE will focus on, among other things, "proper configuration of network storage devices, information security governance generally, and policies and procedures related to retail trading information security. Specific to investment advisers, OCIE will emphasize cybersecurity practices at investment advisers with multiple branch offices, including those that have recently merged with other investment advisers, and continue to focus on, among other areas, governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response." *See* 2019 Examination Priorities, available here.

Though it is hard to know *exactly* what OCIE will focus on, here are some thoughts based upon the telegraph OCIE sent us in its 2019 Examination Priorities:

1. Multiple branch offices/M&A risk: These ideas are related. Multiple branch offices might be under the same letterhead, but likely will have different employees, equipment, and architecture. Most importantly, multiple branch offices need to be monitored 24/7 for anomalies. Sometimes that is easy; sometimes it's hard if the offices opened at different times. How do you monitor 14 branch offices at the same time, for example? The SEC might want to know. Similarly, problems can happen in M&A settings. And distinct issues arise when answering the following enduring questions: Where is my data, what am I storing, and where is it located? Good data governance on the part of the seller will help here. Good due diligence on the buyer side will help, too. Another M&A issue is simply "differences in style." What happens if the buyer's cybersecurity is rated "grade A" but the seller's cybersecurity rated "C minus?" How to harmonize these differences? How much do you spend to do it? And, what happens if the seller already has been breached but doesn't know it? All good questions. All require thorough M&A due diligence.

2. "Governance" comes up several times in the Examination Priorities document as "information security governance" and "governance and risk assessment," which brings up several considerations. If you are a registered investment adviser, do you have the basic policies and procedures you should have, like a privacy policy, an incident response policy, a business continuity policy, a crisis communications policy, and an access-management policy governing who may access the network, and what information they may access? "Governance and Risk Assessment" also could comprise several different points: Does the board regularly meet with management and IT staff to discuss the cybersecurity of the enterprise? What reports does the board regularly receive on the cybersecurity of the enterprise to help fulfill its oversight duty? Does the board participate in or oversee incident response exercises? Finally, does the board require regular vulnerability and compromise assessments so IT staff and management have a firm understanding of where the entity can be hacked or where it is vulnerable to attack?

3. The OCIE document touched on access management policies. They are critical for any organization. An access management policy answers the following questions: (1) who has access to my network, (2) what do they have access to, (3) do they have access to only those areas and only that information required to do their jobs (called least privileged access), and (4) if they leave the firm, is their computer and network access terminated? There is more to access management, but these are the basics.

4. Vendor management is a huge area of concern in corporate America today. What does it generally mean? It means firms and corporations have scores of vendors, consultants, and suppliers. This poses two types of concerns. The first involves situations where such parties have access to the corporate network. If they do have access, (1) who has access, (2) what access do they have, (3) is such access limited or unlimited, and most importantly, (4) what sort of cybersecurity does the vendor have? Good, bad, or totally insufficient? Why does that matter? Because many of the largest breaches ever have occurred when a vendor was hacked and credentials stolen, and then the attacker used those credentials to attack the end user corporation or firm. This happens far too frequently on both the civilian side and the Department of Defense side. Comprehensive, trusted third-party vendor due diligence programs are essential to stop these vendor-related breaches. The second scenario involves vendors who provide or support the firm's network, such as an email archival firm or cloud storage provider. OCIE often seeks to understand what the firm knows about the security and policies of the supporting vendor. What questions were asked before they were hired? What continuing monitoring is conducted to assure good practices at the vendor?

5. Finally, training employees and the c-suite on proper email and social media practices is essential for any corporation or firm. Training board members on good data security practices is essential, too. These programs should be frequent in order to reinforce the need for good security. There is an old saying, "don't click on the link or attachment." That saying is as valid today as it was 10 years ago.

This GT Alert provides but a partial list of what might come up on the Cyber Sweep. While the list is long, nothing is outside the realm of reasonableness.[1] In sum, the SEC is scanning for whether the registered investment adviser, along with its management and board, is focused on privacy, information security, and good cybersecurity practices. Though some of these terms are different, they are all related in that a failure on one area (like cybersecurity) could cause a catastrophic effect throughout the organization and, ultimately, a loss of corporate reputation. It's better to be prepared from the outset by regularly testing your procedures via table top exercises than to suffer a breach or mismanage a hack and lose the faith and trust of your customers and clients.

Author

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

- Paul Ferrillo | +1 212.801.6598 | ferrillop@gtlaw.com
- Ian C. Ballon | +1 650.289.7881 | ballon@gtlaw.com
- Dr. Viola Bensinger | +49 30.700.171.150 | viola.bensinger@gtlaw.com
- Kate Black | +1 415.655.1300 | blackk@gtlaw.com
- Richard M. Cutshall | +1 312.476.5121 | cutshallr@gtlaw.com
- Lori Chang | +1 310.586.3863 | changl@gtlaw.com
- Arthur Don | +1 312.456.8438 | dona@gtlaw.com
- Steven M. Felsenstein | +1 215.988.7837 | felsensteins@gtlaw.com
- Francoise Gilbert | +1 650.804.1235 | gilbertf@gtlaw.com
- David M. Greenberg | +1 212.801.6545 | greenbergdm@gtlaw.com
- Carsten Kociok | +49 30.700.171.119 | carsten.kociok@gtlaw.com
- Carmina Mogollón González | +52 55.5029.0034 | mogollonc@gtlaw.com
- Gretchen A. Ramos | +1 415.655.1319 | ramosg@gtlaw.com
- Radboud Ribbert | +31 (0) 20.301.7333 | ribbertr@gtlaw.com
- Alan N. Sutin | +1 212.801.9286 | sutina@gtlaw.com
- Hans Urlus | +31 (0) 20.301.7324 | urlush@gtlaw.com
- Or your Greenberg Traurig attorney

[1] Indeed, registrants could easily be subject to credential stuffing attacks like other companies have been in 2019, and should consider many of the fixes we have proposed in the past (*see* GT Alert, "Retailers: Protecting Against Credential Stuffing Attacks").