Simpson Thacher

Regulatory and Enforcement Alert

Drawing on Thousands of Exams, OCIE Issues New Cybersecurity and Resiliency Observations

January 28, 2020

For a number of years, the SEC's Office of Compliance Inspections and Examinations ("**OCIE**") has made cybersecurity a key priority in recognition of the risk that cyber threats pose to securities market participants, the financial markets and the economy. As part of this focus, OCIE has published a number of risk alerts concerning cybersecurity. As OCIE explains, "in an environment in which cyber threat actors are becoming more aggressive and sophisticated—and in some cases are backed by substantial resources including from nation state actors—firms participating in the securities markets, market infrastructure providers and vendors should all appropriately monitor, assess and manage their cybersecurity risk profiles, including their operational resiliency."

Yesterday, drawing on thousands of examinations of investment advisers, broker-dealers, and other securities market participants, OCIE issued examination observations related to cybersecurity and operational resiliency practices taken by market participants.

The examination observations focus on specific practices in the following areas:

- Governance and risk management;
- Access rights and controls;
- Data loss prevention;
- Mobile security;
- Incident response and operational resiliency;
- Vendor management; and
- Training and awareness.

This memorandum provides a summary of the examination observations report, which is titled "Cybersecurity and Resiliency Observations" and can be found in full here.

Governance and Risk Management

OCIE observes that effective cybersecurity programs start with the right tone at the top, with senior leaders who are committed to improving their organization's cyber posture. It points out that board and senior leadership at organizations devote their attention to overseeing cybersecurity and operational resiliency programs.

Organizations are also developing and conducting organization-specific risk assessment processes. In addition, organizations are regularly testing and monitoring their programs to validate the effectiveness of their cybersecurity policies and procedures, as well as promptly updating policies and procedures to address any weaknesses.

Access Right and Controls

OCIE discusses the following strategies for managing an organization's access rights and controls:

- **User Access.** Developing a clear understanding of access needs to systems and data, including limiting access to sensitive systems and data and requiring periodic account reviews.
- **Access Management.** Managing user access through systems and procedures that limit access as appropriate; re-certifying users' access rights on a periodic basis; requiring strong, periodically changed, passwords; and utilizing multi-factor authentication ("**MFA**").
- **Access Monitoring.** Monitoring user access and developing procedures that monitor for failed login attempts and account lockouts; properly handling customer requests for user name and password changes as well as procedures for authenticating anomalous or unusual customer requests; and ensuring that any changes are approved and properly implemented, and that any anomalies are investigated.

Data Loss Prevention

Data loss prevention typically includes a set of tools and processes to ensure that sensitive data is not lost, misused, or accessed by unauthorized users. OCIE describes the following data loss prevention measures used by organizations:

- Establishing a vulnerability management program.
- Controlling, monitoring, and inspecting all network traffic to prevent unauthorized or harmful traffic.
- Implementing capabilities that detect threats on endpoints (for example, products that can identify incoming fraudulent communications to prevent unauthorized software or malware from running).
- Establishing a patch management program covering all software and hardware.
- Maintaining an inventory of software and hardware assets, including identification of critical assets and information.
- Using tools and processes to secure data and systems, including encrypting data "in motion" both internally and externally, encrypting data "at rest" on all systems, and implementing network segmentation and access control lists to limit data availability to only authorized systems and networks.
- Creating an insider threat program to identify suspicious behaviors and creating rules to identify and block the transmission of sensitive data.

- Verifying that the decommissioning and disposal of software and hardware do not create system vulnerabilities.

Mobile Security

To address the unique vulnerabilities that mobile devices and applications may create, organizations have, according to OCIE, established policies and procedures for mobile device use and manage mobile device use with mobile device management ("**MDM**") applications or similar technology.

Organizations using a "bring your own device" policy also ensure that the MDM solution works with all mobile phone/device operating systems. Other measures observed by OCIE include implementing security measures, such as requiring MFA for all users; preventing users from printing, copying, pasting or saving information to personally owned devices; and ensuring that data on former employees' devices, or on lost devices, can be remotely cleared.

Incident Response and Operational Resiliency

OCIE observes that incident response plans tend to include the following elements:

- Plans for various scenarios, including procedures that address:
  - timely notification and response if an event occurs;
  - a process to escalate incidents to appropriate levels of management; and
  - communication with key stakeholders.
- Determining and complying with applicable federal and state reporting requirements for cyber incidents or events, such as requirements for public companies to disclose material risks and incidents.
- Designating employees with specific roles and responsibilities in the event of an incident.
- Testing the incident response plan and potential recovery times, using a variety of methods including tabletop exercises and assessing the response after any incident to determine whether any changes to the procedures are necessary.

With respect to operational resiliency, OCIE describes the following strategies:

- Identifying and prioritizing core business services.
- Understanding how individual system or process failure will impact business services.
- Mapping the systems and processes that support business services.
- Developing a strategy for operational resiliency with defined risk tolerances tailored to the organization.
- Maintaining back-up data in a different network and offline.
- Evaluating whether cybersecurity insurance is appropriate.

Vendor Management

With respect to vendor management, OCIE has observed the following practices:

- Establishing a vendor management program to ensure that vendors meet security requirements and that appropriate safeguards are implemented, as well as establishing procedures for terminating or replacing vendors.
- Understanding all vendor contract terms including rights, responsibilities, expectations, and other specific terms to ensure that all parties have the same understanding of how risk and security is addressed.
- Monitoring the vendor relationship to ensure that the vendor continues to meet security requirements and to be aware of changes to the vendor's services or personnel.

Training and Awareness

With respect to cybersecurity training and awareness, OCIE describes the following practices:

- Training staff to implement the organization's cybersecurity policies and procedures.
- Providing specific cybersecurity and operational resiliency training, including phishing exercises to help employees identify phishing emails.
- Monitoring to ensure employees attend training and assessing the effectiveness of training.
- Continuously re-evaluating and updating training programs based on cyber-threat intelligence.

Summary

In sharing these observations from its exams, OCIE encourages securities market participants to review their practices, policies, and procedures for cybersecurity and operational resiliency. "Recognizing that there is no such thing as a 'one-size fits all' approach," OCIE believes that an organization can become more secure by assessing its level of preparedness and implementing some or all of the measures described in the examination observations. OCIE also stated that it will continue to work with organizations to identify and address cybersecurity risks and encourages securities market participants to actively engage regulators and law enforcement in this effort. More broadly, the examination observations signal that cybersecurity and operational resiliency will remain a core priority of OCIE exams for the foreseeable future.

For further information about this Alert, please contact one of the following attorneys or your regular Simpson Thacher contact.

NEW YORK CITY

Thomas H. Bell
+1-212-455-2533
tbell@stblaw.com

Barrie B. Covit
+1-212-455-3141
bcovit@stblaw.com

Brooke E. Cucinella
+1-212-455-3070
brooke.cucinella@stblaw.com

Paul C. Curnin
+1-212-455-2519
pcurnin@stblaw.com

Stephen M. Cutler
+1-212-455-2773
stephen.cutler@stblaw.com

Nicholas S. Goldin
+1-212-455-3685
ngoldin@stblaw.com

Olga Gutman
+1-212-455-3522
ogutman@stblaw.com

Jason A. Herman
+1-212-455-3697
jherman@stblaw.com

Jonathan A. Karen
+1-212-455-3274
jkaren@stblaw.com

Parker B. Kelsey
+1-212-455-3877
pkelsey@stblaw.com

Steven R. Klar
+1-212-455-2988
steven.klar@stblaw.com

Joshua A. Levine
+1-212-455-7694
jlevine@stblaw.com

Michael J. Osnato, Jr.
+1-212-455-3252
michael.osnato@stblaw.com

Glenn R. Sarno
+1-212-455-2706
gsarno@stblaw.com

Peter P. Vassilev
+1-212-455-2319
peter.vassilev@stblaw.com

Benjamin Wells
+1-212-455-2516
bwells@stblaw.com

Michael W. Wolitzer
+1-212-455-7440
mwolitzer@stblaw.com

Jonathan K. Youngwood
+1-212-455-3539
jyoungwood@stblaw.com

Allison Scher Bernbach
+1-212-455-3833
allison.bernbach@stblaw.com

Manny M. Halberstam
+1-212-455-2388
manny.halberstam@stblaw.com

HONG KONG

Adam C. Furber
+852-2514-7670
afurber@stblaw.com

Adam Goldberg
+852-2514-7552
adam.goldberg@stblaw.com

HOUSTON

James M. Hays
+1-713-821-5663
james.hays@stblaw.com

LOS ANGELES

Thomas A. Wuchenich
+1-310-407-7505
twuchenich@stblaw.com

LONDON

Gareth Earl
+44-(0)20-7275-6542
gareth.earl@stblaw.com

Jason Glover
+44-(0)20-7275-6525
jglover@stblaw.com

Robert Lee
+44-(0)20-7275-6388
robert.lee@stblaw.com

Daniel Lloyd
+44-(0)20-7275-6498
dlloyd@stblaw.com

Seema Shah
+44-(0)20-7275-6455
seema.shah@stblaw.com

PALO ALTO

Stephen P. Blake
+1-650-251-5153
sblake@stblaw.com

Robert Guo
+1-650-251-5127
rguo@stblaw.com

James G. Kreissman
+1-650-251-5080
jkreissman@stblaw.com

Michael J. Nooney
+1-650-251-5070
mnooney@stblaw.com

WASHINGTON, D.C.

David W. Blass
+1-202-636-5863
david.blass@stblaw.com

Rajib Chanda
+1-202-636-5543
rajib.chanda@stblaw.com

Crystal L. Frierson
+1-202-636-5510
cfrierson@stblaw.com

David J. Greene
+1-202-636-5857
david.greene@stblaw.com

Jeffrey H. Knox
+1-202-636-5532
jeffrey.knox@stblaw.com

Cheryl J. Scarboro
+1-202-636-5529
cscarboro@stblaw.com

John Terzaken
+1-202-636-5858
john.terzaken@stblaw.com