

2024 Investment Adviser Compliance Conference

MARCH 6-8 / WASHINGTON, DC

EFFECTIVE STRATEGIES & BEST PRACTICES

Cybersecurity for Smaller and Medium Firms

Gordon Eng, SKY Harbor Capital Management, LLC

Christian Kelly, CISSP, Xantrion

Joseph Mannon, Vedder Price P.C. (MODERATOR)

1

1



2024 Investment Adviser
Compliance Conference

EFFECTIVE STRATEGIES
& BEST PRACTICES

Disclaimer

This presentation is intended for educational and discussion purposes only, and nothing stated today whether in writing or verbally shall constitute legal advice.

The content of this presentation and comments expressed by the moderator and each panelist are solely their personal perspectives, views, and opinions and do not represent the perspectives, views, opinions or policies of their affiliated entities.

2

2



2024 Investment Adviser
Compliance Conference

EFFECTIVE STRATEGIES
& BEST PRACTICES



Agenda

- SEC's Proposed Cybersecurity Risk Management Rules
- Recent Division of Examinations Risk Alerts and Division of Enforcement cases
- Reasonably Designed Cybersecurity Policies and Procedures
- Practical Practice Pointers

3

3



2024 Investment Adviser
Compliance Conference

EFFECTIVE STRATEGIES
& BEST PRACTICES



Cybersecurity: why all the fuss?

Only a matter of time before Threat Actors will see smaller and medium sized financial firms as easier targets than the big banks/firms that have substantial cybersecurity budgets and employ large staffs of technologists.

4

4



Cybersecurity: an existential threat

Significant Cyber Incidents can result in:

- Significant financial and operational harm (regulatory sanctions, fines, lawsuits, remediation expenses, increased cyber insurance premiums)
- Reputational Harm can be irreparable for smaller and medium size firms
- Loss of client confidence in firm's ability to act as fiduciary of client assets

5

5



The CIA of Cybersecurity

No presentation of Cybersecurity would be complete without a reminder that, the essential core of the cybersecurity is data security, which in turn rests on three pillars:

- Confidentiality
- Integrity
- Availability

Every aspect cybersecurity touches one or more to these three pillars directly or indirectly, and keeping these pillars in mind while traveling through the topic may be a helpful focal point.

6

6



The Proposed Rule

Published in the Federal Register on March 9, 2022, vol. 87, No. 46, at 13524 entitled: Cybersecurity Risk Management for Investment Adviser, Registered Investment Companies, and Business Development Companies. The Proposed Rule has not yet been enacted.

7

7



Scope of the Proposed Rule

- RIAs (and their private funds), Registered Funds and BDCs
- Adopt and implement written cybersecurity policies and procedures reasonably designed to address cybersecurity risks and reviewed no less frequently than annually
- Required to report promptly to the SEC but not less than 48 hours after a “significant cybersecurity incident(s)” has occurred or is occurring
- New IAA and ICA Disclosure Forms and Recordkeeping Rules

8

8



Proposed Rule Reporting Obligation

Advisers would be required to report significant cybersecurity incidents to the Commission, including on behalf of a client that is a RIC, or a BDC, or a private fund (each a “covered client”) that experiences a significant cybersecurity incident.

Any RIA or any adviser required to be registered with the SEC as an investment adviser would be required to report on proposed Form ADV-C promptly, but in no event more than 48 hours, after having a *reasonable basis* to conclude that a significant adviser cybersecurity incident or significant fund cybersecurity incident had occurred or is occurring. (emphasis added)

9

9



Confidential Treatment (for now)

The SEC acknowledged in the Proposed Rule that public disclosure of an adviser’s significant cybersecurity breach “harm an adviser’s or fund’s ability to mitigate or remediate the cybersecurity incident, especially if it is ongoing.

“Accordingly, our preliminary view is that Form ADV– C should be confidential given that public disclosure is neither necessary nor appropriate in the public interest or for the protection of investors.” Proposed Rule at 13539.

10

10



Follow Up Reporting Obligation

Proposed rule 204–6 would also require advisers to amend any previously filed Form ADV–C promptly, but in no event more than 48 hours, after information reported on the form becomes materially inaccurate; if new material information about a previously reported incident is discovered; and after resolving a previously reported incident or closing an internal investigation pertaining to a previously disclosed incident.

11

11



What Is A Significant Cybersecurity Incident?

Under the proposed rule, “a significant adviser cybersecurity incident is a cybersecurity incident, or a group of related incidents, that significantly disrupts or degrades the adviser’s ability, or the ability of a private fund client of the adviser, to maintain critical operations [broadly defined in FN 60], or leads to the unauthorized access or use of adviser information, where the unauthorized access or use of such information results in: (1) Substantial harm to the adviser, or (2) substantial harm to a client, or an investor in a private fund, whose information was accessed.”

12

12



The SEC's Concerns

- The “staff continues to observe that certain advisers and funds show a lack of cybersecurity preparedness, which puts clients and investors at risk.”
- The staff is “concerned that clients and investors may not be receiving sufficient cybersecurity-related information, particularly with respect to cybersecurity incidents to help ensure they are making informed investment decisions.”

The Proposed Rule at 13525

13

13



Cybersecurity as a Fiduciary Duty

The proposed Cybersecurity Rule if enacted will be promulgated under 17 CFR 275.206(4)-9 of the IAA and under 17 CFR 270.38a-2.

As a reminder, the proposed rule is promulgated under Section 206 of the IAA, Prohibited Transactions by Registered Investment Advisers, which imposes a fiduciary duty on RIAs by operation of law per the 1963 SCT case SEC v. Capital Gains Research Bureau, Inc.

14

14



2024 Investment Adviser
Compliance Conference

**EFFECTIVE STRATEGIES
& BEST PRACTICES**



Current Legal and Regulatory Framework

“An adviser’s fiduciary obligation to its clients includes the obligation to take steps to protect client interests from being placed at risk because of the adviser’s inability to provide advisory services,” which “include steps to minimize operational and other risks that could lead to significant business disruptions or a loss or misuse of client information,” . . . “Thus, advisers should take steps to minimize cybersecurity risks in accordance with their fiduciary obligations.” Proposed Rule at 13526.

15

15



2024 Investment Adviser
Compliance Conference

**EFFECTIVE STRATEGIES
& BEST PRACTICES**



SEC Resources

16

16



2024 Investment Adviser
Compliance Conference

**EFFECTIVE STRATEGIES
& BEST PRACTICES**



- OCIE Cybersecurity and Resiliency Observations (2019)
 - <https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf>
- Observations from Cybersecurity Examinations (2017)
 - <https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf>
- SEC Announces Three Actions Charging Deficient Cybersecurity Procedures
 - <https://www.sec.gov/news/press-release/2021-169>

17

17



2024 Investment Adviser
Compliance Conference

**EFFECTIVE STRATEGIES
& BEST PRACTICES**



Reasonably Designed Cybersecurity Policies and Procedures

18

18



What the SEC believes:

“We believe that advisers and funds should be required to adopt and implement policies and procedures that **address a number of elements** to increase the likelihood that they are prepared to face a cybersecurity incident (whether that threat comes from an outside actor or the firm’s personnel), and that investors and other market participants are protected from a cybersecurity incident that could significantly affect a firm’s operations and lead to significant harm to clients and investors.” (emphasis added)
Proposed Rule at 13527.

19

19



NB: What California believes:

In February 2016, then-California Attorney General Kamala D. Harris wrote in the 2016 California Data Breach Report:

“The 20 [now 18] controls in the [CIS’s] Critical Security Controls identify a *minimum* level of information security that all organizations that collect or maintain personal information should meet. The *failure to implement all the Controls* that apply to an organization’s environment *constitutes a lack of reasonable security.*” (emphasis added)

20

20



Accountability

P&P should designate the person(s) who shall implement and oversee the effectiveness of the firm's cybersecurity policies and procedures. CCO's extra job?

The Proposed Rule permits the use of third-party cybersecurity risk management services ("MSPs"), but Investment Advisers are responsible to exercise appropriate oversight. What does appropriate oversight look like?

21

21



Liability Considerations

Will CCOs or COOs of small and medium firms embrace the added role of CISO after recent enforcement action against the former SolarWinds CISO?

Is the paradigm of CCO liability portable to the CISO role? See Vedder Price PC, Nov. 24, 2023, comment on CCO Liability

(affirmatively participate in misconduct, mislead regulator, wholesale failure to perform)

22

22



Duty of Oversight

- Most smaller and medium size firms outsource cybersecurity to Managed Service Providers (“MSP”), but you should have sufficient knowledge to exercise reasonable oversight.
- Review closely your contracts, MSAs, and SOWs and understand each component of your MSP’s services and tools employed to address cybersecurity concerns.
- Ask your MSP how your current network and cybersecurity infrastructure reflects the principle of “Defense-in-Depth”?

23

23



Cybersecurity: Getting Up to Speed

- Regulatory involvement in managing cybersecurity risk, now more than ever, merits the attention of executive management and the Boards of both public and private companies.
- Either upstream or downstream relationships with public companies can trigger an incident response and/or regulatory reporting obligation, which may implicate or directly involve a private company.
- Education, Awareness, and Training: many available resources

24

24



Essential First Steps

- Conduct a Threat Vulnerability Assessment
- Rank the Risks (probability of occurrence and impact of occurrence)
- Allocate Resources and establish Partnerships (internal and external)
- Build consensus among senior management and internal stakeholders and balance risk management with business priorities

25

25



Risk Frameworks and Assessment Methodologies

- Prepare the firm to deal with and categorize cyber risks
- Select Controls – NIST pub. 800-53 ver. 5; Center for Internet Security Critical Security Controls v.8; ISO/IEC 27001
- Implement and Assess Controls
- Authorize and drive accountability
- Monitor and adjust accordingly (consider KPIs)

26

26



KEY Elements in Cybersecurity P&P

- Risk Assessment
- Data Protection (privacy)
- Secure Configuration of Enterprise Assets and Software
- Account Management
- Access Control Management
- Continuous Vulnerability Management
- Audit Log Management
- Email and Web Browser Protection
- Malware Defense
- Data Recovery
- Source: Center for Internet Security Critical Security Controls V. 8

27

27



And there's more!

- Network Infrastructure Management
- Network Monitoring and Defense
- Security Awareness and Skills Training – a culture of cybersecurity awareness and vigilance
- Service Provider Risk Management
- Application Software Security
- Incident Response
- Penetration Testing

28

28



Center for Internet Security Critical Controls

The foregoing series of Key Elements of Cybersecurity P&P comprise virtually all 18 controls* (formerly 20 Controls in Version 7 until May 2021) set forth in the Center for Internet Security (“CIS”) Critical Security Controls, Version 8, a widely-recognized and accepted cybersecurity risk framework.

*The CIS’s “Inventory and Control of Enterprise Assets” and “Inventory and Control of Software Assets” were compressed as “Risk Assessment” in the prior slide.

29

29



Key Cybersecurity Principles

- Defense-in-depth
- Least privilege or Zero Trust Network Access (“ZTNA”)
- Understand your firm’s “Attack Surface” by inventorying and controlling all endpoints, especially if you are an all or hybrid distributed workforce (WFH) business model.
- Continuous Vulnerability Management
- Robust and resilient Incident Response

30

30

National Institute of Standards and Technology

NIST Cybersecurity Framework (“CSF”) five core functions:

- Identify
- Protect
- Detect
- Respond
- Recover

See also NIST publication 800-53 Rev 5, Security and Privacy Controls for Information Systems and Organizations available at: <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>. Last visited: Feb. 7, 2024, sets forth 20 “families” of cybersecurity controls including P&P, specific controls, control enhancements, and detailed discussion.

31

31

A closer look at Vulnerability Analysis

Vulnerability analysis consists of a tools to detect, mitigate, and remediate cybersecurity threats and vulnerabilities:

- Endpoint Detection and Response Systems (“EDR”)
- Network Detection and Response Systems (“NDR”)
- Intrusion Detection Systems (“IDS”) and Intrusion Prevention System (“IPS”)

32

32



Looking up to the Cloud

Size notwithstanding, our industry is undergoing a digital transformation, and much of it is led by migrating significant IT and Communication infrastructure to “the cloud” (e.g., AWS, Azure, Google, or private clouds).

With pandemic legacy WFH or hybrid structures, centralized cybersecurity command and controls are now a necessary part of a firm’s cybersecurity infrastructure.

33

33



Centralized Command and Control

The former model of a physical office defended by a physical or electronic/firewall perimeter protecting all those inside from outside threats is an outdated and arguably a dangerously obsolete cybersecurity model.

A firm (or its MSP) must be able to remotely configure, maintain, patch and update security protocols to multiple endpoints (located anywhere and everywhere) simultaneously and in a timely way.

34

34



Weaving in SIEMS and SOCs

- Security Information and Event Management Systems (SIEMs) – a single pane of glass to monitor the attack surface with automated alerts
- Security Operations Center (SOC) – a team to detect, respond and recover
- Data Loss Prevention Systems – detect potential exfiltration
- Network Traffic Analysis – detect DDoS attacks

35

35



Intrusion Detection Frameworks

MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge), is a structured matrix of tactics, techniques, and procedures (“TTPs”) used by threat actors to find, infiltrate, and impact networks and data by impairing, damaging or destroying the confidentiality, integrity and availability of a firm’s data. See <https://attack.mitre.org/matrices/enterprise/>

36

36



What is a Significant Cybersecurity Event?

Factors in the Calculus Determining a Significant Cybersecurity Incident:

- Did the data breach put the firm or any employees or clients at risk?
- Severity, Scope, and Impact on CIA data privacy triad
- Nature of the Compromised Data (PII, PCI-DSS, IP, bank a/c)
- Regulatory, Legal and Insurance Considerations
- Disclosure Obligations: regulators, law enforcement, stakeholders, public
- Financial Impact/Business Impairment

37

37



Severity, Scope and Impact

- Duration of Incident (still ongoing? How long until discovered? APT? Time needed to determine significance?)
- Nature of the data breach? Quality and Quantity, Exfiltrated, altered or corrupted Impaired Availability (Ransomware)
- Impact on operating business (degree of impairment or impediments to trading, investing, reporting, sales, back-office operations, risk management, marketing, or compliance functions? Will major business units be taken offline? For how long?)

38

38



Nature of Compromised Data

- PII notice obligations to affected individuals – each state has its own laws and rules
- Unclassified Controlled Information – subject to applicable law, regulation, and government policies although not classified
- Was the data encrypted? If so, how secure was the cypher used?

39

39



Regulatory, Legal, and Insurance

- Have any statutory or regulatory mandates been violated? (e.g., GLBA, CCPA, HIPAA, GDPR)
- Have any contractual obligations been triggered requiring disclosure? (e.g., NDAs covering another party's confidential information)
- Has a claim been filed under a claims made cyber insurance policy? Should a filed claim be presumed significant?

40

40



A Reasonable Basis to Report

The Proposed Rule highlights that the 48-hour reporting obligation is triggered as soon the RIA has a “reasonable basis” to conclude that a significant adviser or fund cybersecurity incident has occurred or is occurring with respect to itself or any of its clients that are covered clients.

“In other words, an adviser must report within 48 hours after having a reasonable basis to conclude that an incident has occurred or is occurring, and not after definitively concluding that an incident has occurred or is occurring. The 48-hour period would give an adviser time to confirm its preliminary analysis and prepare the report while still providing the Commission with timely notice about the incident.” Proposed Rule at 13537.

41

41



Financial Impact: ex ante and ex post

- Ex ante public disclosure: what is the financial impact on the business in containing and remediating the incident?
- Ex post financial consequences of disclosing to external stakeholders and the public? Loss of market share, client assets, redemptions; public relations, legal, insurance fees in handling public fallout
- Ransomware and other threats to release confidential data

42

42



External Experts

- Financial impact of retaining forensic, legal, accountants, and other consultants?
- Is an internal investigation needed? If so, who should conduct it? What will be its scope? Who will be data custodians targeted for discovery? Written or oral report? Employee sanctions within scope?
- Maintaining and preserving attorney client privilege – consider off band communication channel if your client is a publicly-owned entity with statutory obligations to disclose internal communications

43

43



Additional Reporting Considerations

Law Enforcement

- Report Ransomware attacks to the FBI's Internet Crime Complaint Center (IC3)
- Cybersecurity & Infrastructure Security Agency – incident reporting system
- U.S. Secret Service

44

44



Practical Practice Pointers - Policies

- Before embarking on writing your firm's Cybersecurity Policies and Procedures consider starting with a template.
 - The IAA has Cybersecurity Policies and Procedures templates available to its members!
- Review and revise BCP-DR Policies and Procedures as part of the exercise of adopting and implementing written cybersecurity policies and procedures

45

45



Practical Practice Pointers - Vulnerability Management

- Enforce centralized and timely patch management on endpoints and servers
- Update firmware on all devices and network appliances
- Require your tech staff or MSP to provide vulnerability reports using the Common Vulnerability Scoring System (CVSS)
- Critical or High CVSS scores should be addressed in a timely fashion (e.g., could be false positives) or remediated
- Retain a qualified service provider reasonably independent of your MSP to perform a Penetration Test at least annually

46

46

Practical Practice Pointers - Identity

- Employ Multi-Factor Authentication on **all** critical apps
- Utilize Single Sign On to secure and centralize logins
- Monitor and alert on abnormal identity behavior
- Practice least privilege and strictly limit privileged access to sensitive servers and data bases (e.g., active directory). SQL data bases should be configured “read only” for general use and availability with only limited privileged users able to read and write data.
- Practice Defense-in-depth: backup data frequently and backup the backup
- Label data according to degree of confidentiality and treat accordingly

47

47

Practical Practice Pointers - Email

- Exercise caution upon receipt of unsolicited, unexpected or suspicious emails; inquire if your email servers have installed DKIM, DMARC, and SPF.
- Install a strong spam filter with advanced phish and spoof protection
- BOLO for sophisticated phishing attempts and social engineering
- Utilize a security awareness training and phish testing program

48

48



Practical Practice Pointers - Network

- Configure Firewalls according to your risk appetite
- If feasible, consider establishing network segmentation to segregate sensitive company-related network traffic from other less sensitive (e.g., DMZ) or non-company traffic
- Be aware that IoT devices can be vulnerability vectors (e.g., printers, webcams, remote thermostats)

49

49



Practical Practice Pointers - Web

- Always be sure you're on the intended site before entering any information.
- Be cautious about websites that do not have a valid certificate issued by a trusted authority, which means information (such as passwords or credit cards) will be securely sent to the site and cannot be intercepted. How can you tell?
- Exercise extreme caution of Microsoft Office attachments that prompt users to enable macros
- Apply symmetric encryption whenever possible (e.g., password protect sensitive documents when transmitting over the internet)

50

50



Practical Practice Pointers - Endpoints

- Before discarding old computers ensure that all data on the equipment is professionally wiped
- Unless you can afford in-house expertise, ensure that your MSSP is able to remotely maintain, monitor, configure, patch, access, re-boot, and if needed, wipe data on all your employee endpoints
- Always Log out of company workstations when done or when absent

51

51



Practical Practice Pointers - Vendor Due Diligence

- Service Providers: inquire and request summary of their BCP-DR policies and procedures; critical suppliers should submit an annual SOC audit report covering internal controls and cybersecurity readiness
- Any service provider with access to your network must be thoroughly and regularly vetted and comply with the same company policies and procedures that apply to employees

52

52



Practical Practice Pointers - Cyber insurance

- Review and update your firm's point of contact with your cybersecurity insurer and be ready to contact and notify the carrier and insurance broker in case an incident warrants filing a claim
- Cyber insurers often provide additional services and features to mitigate risks – read the policy and take advantage of them
- Unless you have in-house expertise, leverage your insurance broker to help you to fully understand the coverage, the retention amounts, and especially the exclusions
- Review and update your firm's point of contact with your MSP and be prepared to respond in the event of a cyber incident (i.e., BCP-DR).

53

53



Questions?

54

54

2024 / Investment Adviser Compliance Conference

MARCH 6-8 / WASHINGTON, DC

**EFFECTIVE STRATEGIES
& BEST PRACTICES**

IAA