OVERSEEING CYBERSECURITY: ENHANCING THE BOARD REPORTING FRAMEWORK

ROPES & GRAY

July 25, 2018

Brief recap on Board's role

- No single source of obligation
- Oversight of compliance program
- Continued evolution

Areas to safeguard

- Sensitive data
  - Material business information
    - Trading strategies, holdings, real-time investments
  - Personal information
    - Shareholder accounts
- Systems integral to operations/access
  - Ability to buy/sell holdings
  - Ability for shareholders to buy/sell interests in the funds
  - Ability for service providers to provide services (e.g., custody, transfer agency, determination of NAV, fund administration, valuation)

Service providers on which to focus

- First line: investment adviser, administrator (if different than adviser), subadvisers, custodian, transfer agent
- Second line: pricing vendors, liquidity risk management vendors, middle/back-office providers, distributor, third-party vendors (i.e., vendors of vendors)
- "Risk ranking" of vendors
  - Importance of vendor to operations/compliance
  - Sensitivity and volume of data held
  - Level of scrutiny

Board evaluation and expectations of cyber preparedness

- Expertise of individual(s) responsible for cybersecurity
- Reports that show evidence of a robust program that has been tailored with fund-specific issues in mind
- Process for appropriate notifications to the Board of a breach/material incident
- Cyberinsurance coverage

Board reporting: gating issues

- Who is responsible for preparing the report for the Board?
- Who is responsible for contributing to the report to the Board?
- Who on the Board will receive the report?

Board reporting: frequency

- Initially
- Annually?
- Quarterly?
- Part of 15(c) process?

Board reporting: initial report

- Cybersecurity risk management framework
  - Governance and key personnel
  - Framework for the risk management program -- policies, procedures and technology
  - Cybersecurity priorities and roadmap for new initiatives
- Risk assessment tailored to the funds
  - Process for identifying risks that are relevant to the funds
  - Identification and inventory of at-risk information elements and operational systems
- Program of controls to address the identified risks
  - Description of how the adviser addresses risk areas for the funds
  - Program of testing and assessment of these cybersecurity controls, including frequency of testing and how the adviser evaluates and addresses gaps identified

Board reporting: initial report (cont.)

- Business continuity and disaster recovery
- Incident response planning
  - Key personnel and pre-approved providers (outside counsel and forensics firm)
  - Relevant policies, procedures and technology
  - Description of “table top” or other practice exercises
  - Overview of how incidents affecting the funds will be handled and reported to the Board
- Status of training
  - Description of trainings (on-boarding, annual, periodic, role-specific, adviser personnel, vendor personnel)

Board reporting: initial report (cont.)

- Overview of vendor management program
  - Identification of key vendors to the funds
  - Method of due diligence and evaluation of risks to the funds
  - Risk-ranking of vendors and methodology for the ranking
  - Treatment of vendors depending on risk-ranking
  - Ongoing monitoring and review of vendors
- Status of cyberinsurance
  - Description of policy as it is relevant to the funds
    - Who is the holder, who is covered, what coverage is provided and not provided

Board reporting: annual report

- Status of the cybersecurity risk management framework
  - Updates on governance structure and key personnel, policies, procedures and technology changes
  - Status of cybersecurity priorities and roadmap for new initiatives in coming year relevant to the funds
- Status of the risk assessment tailored to the funds
  - Date of last assessment and relevant findings
  - Status of, and updates to, the inventory of at-risk information elements and operational systems
- Status of the program of controls
  - Status of access rights and controls, data loss prevention, etc.
  - Status of testing and assessment program, including assessments performed since last report, and how identified gaps are being addressed

Board reporting: annual report (cont.)

- Updates to the business continuity and disaster recovery plans
- Status of incident response planning
  - Updates to key personnel and pre-approved providers policies, procedures and technology
  - Status of “table top” or other practice exercises conducted since last report
  - Description of any recent incidents relevant to the funds
- Status of vendor management program and efforts since last report
  - Status of due diligence and risk-ranking of vendors
  - Results of any assessments and resulting plans of action
    - Whether any key service providers identified as having elevated risk on the prior annual report continue to have an elevated risk ranking. If so, provide a status report on efforts to mitigate the risk, and due dates/responsible parties
  - Update regarding ongoing monitoring and review of vendors

Board reporting: annual report (cont.)

- Updates on training
  - Describe any changes to the training program
    - Identify what percentage of employees received the required trainings in the last annual period
    - Identify any service providers that did not receive the required trainings in the last annual period
- Status of cyberinsurance
  - Describe any changes anticipated for the next policy period
- Cybersecurity threat trends
  - What does management do to stay abreast and ahead?
  - Mitigation controls and efforts
  - Examples of non-material breaches/incidents during the year, how they were addressed and lessons learned

Board reporting: quarterly report

- Deeper dives on selected issues from the initial or annual reports
- Legal and regulatory developments
- Cybersecurity threat trends and status of any counter measures
  - Breaches/incidents since prior report
- Update on the matrix of at-risk information elements and operational systems, including risk ranking and relevant vendors
- Changes/enhancements to program since prior report (including staffing changes)

Appendix

[Template]

Cybersecurity Board Update - Quarterly

Table of Contents

- Legal/Regulatory Developments
- Cybersecurity Threat Trends
- Risk Assessments
- Cybersecurity Initiatives

Legal/Regulatory Developments

- [Any significant legal or regulatory developments impacting the funds industry in the cybersecurity space since last update]

Cybersecurity Threat Trends: Industry

- [Describe high-profile threats and recent incidents within the industry]
  - [Leverage information from the FS-ISAC, https://www.fsisac.com/]
- [Lessons learned from recent threats and incidents]

[Example] Cybersecurity Threat Trend – Office 365

- Attacks exploiting Microsoft Office 365
  - Attacker steals employee credentials through phishing emails
  - Impersonates firm in communications with third-parties
- *Lessons Learned*:
  - Implement multi-factor identification on Office 365
  - Consider ways to securely communicate with key third-parties

Cybersecurity Threat Update: Firm

- [Describe recent threats and incidents at the firm]
- [How did the firm respond?]
- [Lessons learned]

Summary Risk Assessments

- [Update “heat map” of at-risk information]
- [Update “heat map” of vendor risk rankings]
- [Priorities for improvement]

[Example] Risk Assessments – At-Risk Information

At-risk information/systems	Relevant vendor/third party	Inherent risk (High/Medium /Low)	Risk rating (High, Medium or Low)/risk trend	Explanation of basis for ratings/comments
Shareholder information	[transfer agent, distributor]	[High]	[Medium/→]	[While inherent risk is high based on the negative consequences if there is a breach that exposes non-public shareholder information ("high" impact score), given our assessment of the strength of the transfer agent's cybersecurity program (assessment last performed 6/2018) and the distributor's cybersecurity program (assessment last performed 1/2018), we believe that the risk level is medium.]
Portfolio holdings	[adviser, custodian]			
Striking NAV	[administrator, custodian, pricing services]			
Trade orders	[trading platforms, adviser's trading desk]			
Potential investment acquisitions/dispositions	[adviser, subadvisers]			
Website that accepts purchase/redemption requests	[adviser, website hosting company]			

[Example] Risk Assessments - Vendors

Vendor/At-Risk Information or System	Testing	Date	Status
Vendor 1/Trading Data	Site Visit	Q1 2018	**Medium**
Vendor 2	Questionnaire	Q4 2017	**Low**
Vendor 3	Site Visit	Q2 2018	**High**
Sub-adviser 1	Questionnaire	Q2 2018	**Low**
Sub-adviser 2	Questionnaire	Q2 2018	**Low**
Sub-adviser 3	Questionnaire	Q2 2018	**Medium**
Sub-adviser 4	Questionnaire	Q2 2018	**Low**

New Vendor

- [Describe services provided]
- [Describe nature of risk to funds]
- [Describe diligence conducted]
- [Describe protections in place to manage risk]

High Risk Vendors

- [Describe services provided]
- [Describe nature of risk to funds]
- [Describe any additional diligence organization will conduct]
- [Describe current protections in place to manage risk]
- [Describe any additional initiatives to manage risk]

Update on Current Cybersecurity Initiatives

- [Provide update on recent initiatives from past presentations, including description and status, as well as new initiatives identified]
- [Describe recent accomplishments]
- [Describe current priorities]
- [Consider highlighting a few key initiatives in separate slides]

New Cybersecurity Initiatives

- [Update on new initiatives and changes to cybersecurity program, including changes to people, processes and technology]

[Example] New Cybersecurity Initiatives

Capability	Project /Program Description	Schedule (start – end)
Security Governance, Risk, and Compliance	Data classification: Identify "crown jewels" and other sensitive data	May 2018 – August 2018
	Phishing training exercise	June 2018 – September 2018
Identity and Access Management	Creating portal for shareholder communications	June 2018 – August 2018
	Automation of access reviews	May 2018 – December 2018
Incident Response	John Smith hired to lead incident response team	April 2018
	Conduct Table Top exercise involving IT security and senior management Engage outside counsel to prepare and facilitate exercise	May 2018

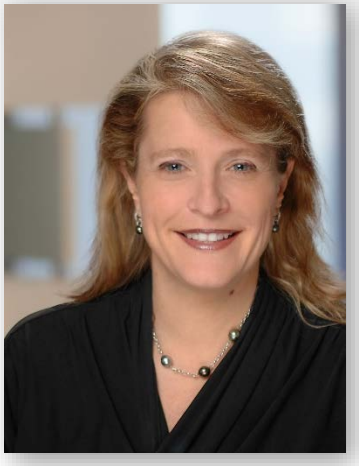
QUESTIONS?

Paulita Pike

PRACTICE

Paulita is a partner of the firm's Investment Management Practice based in Chicago. She represents mutual funds or their boards as well as investment advisers and fund service providers throughout the country. Paulita advises her clients on a broad range of issues including governance structures and practices, compliance issues and D&O/E&O matters. She counsels clients in relation to committee structures and functions, communications with the press, self-evaluations and industry "best practices," fund service provider contracts and filings with the Securities and Exchange Commission, fund mergers and "manager-of-managers" arrangements. Paulita also advises clients on regulatory investigations and inquiries, and on matters arising from the Investment Company Act of 1940 and the Investment Advisers Act of 1940. As concerns surrounding data security have heightened, Paulita advises mutual fund managers, investment advisers and fund boards on cybersecurity issues and best practices for data protection.

Paulita is an Adjunct Professor at Notre Dame Law School and Northwestern Pritzker School of Law, where she teaches courses, along with Paul Dykstra, on mutual fund regulation.



Partner, Chicago
Paulita.Pike@ropesgray.com
312.845.1212

EDUCATION

- JD, University of Notre Dame Law School
- BA, University of Notre Dame

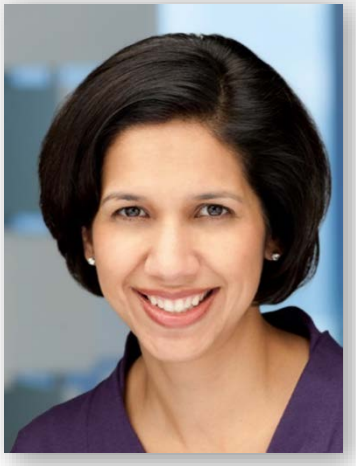
AWARDS

- Mutual Fund Awards Hall Of Fame Inductee, *Fund Directions'* Mutual Fund Industry Awards (2017)
- *Chambers USA: America's Leading Lawyers for Business* (2015-2018)
- Independent Counsel of the Year, *Fund Directions'* Mutual Fund Industry Awards (2013 and 2008)
- *Legal 500 US* (2014-2016, 2018)
- *The Best Lawyers in America* (2006-2018)

Elizabeth Reza

PRACTICE

Elizabeth is a partner of the firm's Investment Management Practice based in Boston. Elizabeth counsels asset managers on regulatory issues that affect the creation and operation of registered investment companies, including the development, organization and offering of new funds; the creation and implementation of compliance programs; and the preparation and review of disclosure in offering documents, shareholder communications, and advertising materials. Elizabeth also regularly advises independent directors regarding their oversight of fund complexes and the establishment of effective governance structures and practices.



Partner, Boston
Elizabeth.Reza@ropesgray.com
617.951.7919

EDUCATION

- JD, Columbia University School of Law
- BA, Columbia College, Columbia University

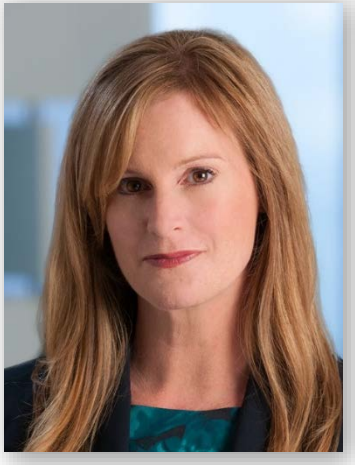
AWARDS

- *Chambers USA: America's Leading Lawyers for Business*, Up & Coming Lawyer (2016-2018)
- *IFLR1000*: The Guide to the World's Leading Financial Law Firms, Rising Star (2014-2018)
- Columbia Law School Latino/a Law Students Association, Distinguished Alumna Award (2011)

Heather Egan Sussman

PRACTICE

Heather Egan Sussman is a partner and co-head of the Privacy & Cybersecurity Practice Group, based in Ropes & Gray's Boston office. Her practice focuses on privacy, cybersecurity and information management. Heather has vast experience counseling a wide range of clients, including mutual fund managers, investment advisers and fund boards, on privacy and cybersecurity issues relevant to their industries. She builds cybersecurity, incident response programs from the ground up, leads table top exercises and helping firms to reduce the risk of a cybersecurity incident and prepare to respond in the event of one. She has performed privacy, security and vendor risk management assessments for investment advisers, mutual fund managers and fund boards. Heather has managed complex security incidents affecting banks, investment firms, asset managers and advisers, overseeing teams of lawyers and outside security professionals helping these firms successfully investigate, remediate and notify relevant individuals, government agencies and insurance companies regarding the incident, pursuant to the law. She works with security firms to help clients reduce the risk of a cybersecurity incident by conducting privileged and confidential red or purple team assignments, penetration tests and other targeted risk assessments.



Partner, Boston
Heather.Sussman@ropesgray.com
617.951.7125

EDUCATION

- JD, Boston College Law School, 2000
- BA, *magna cum laude*, University of Massachusetts Dartmouth, 1996

AWARDS

- *Best Lawyers* (2018)
- *Cybersecurity Docket's "Incident Response 30"* (2016; 2018)
- *Chambers USA*
- *The Legal 500 United States*