September 20, 2018

Cybersecurity: Considerations for Fund Directors

IDC Webinar

Panelists

Joanne Pace, Moderator
Independent Director
Oppenheimer Funds

Janine Comstock
Senior Vice President and Chief Security Officer
MFS Investment Management

Bruce G. Leto
Partner and Co-Chair, Investment Management Group
Stradley Ronon Stevens & Young, LLP

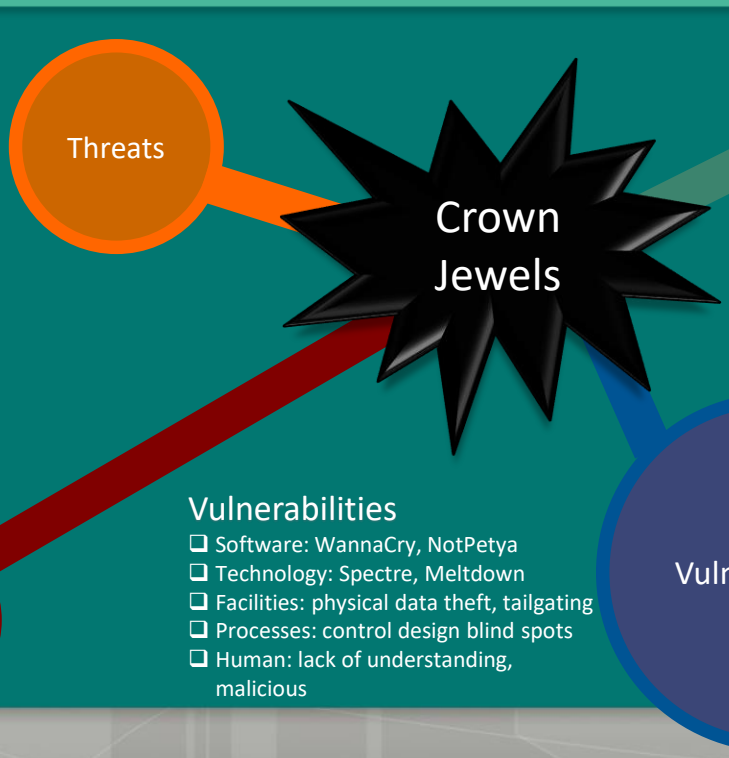
Outline for Today's Webinar Discussion

- Potential cyber threats and risks for funds
- Fund board oversight
- What should fund boards do to engage?
- Framework for board-adviser discussion
- Resources for fund directors

IDC
INDEPENDENT DIRECTORS COUNCIL

Potential Cyber Threats and Risks for Funds

Threats
- ❑ Phishing emails
- ❑ Social Engineering tactics
- ❑ Ransomware
- ❑ Distributed denial of service (DDoS)
- ❑ Botnets and malware
- ❑ High risk users
- ❑ Privilege access escalation
- ❑ By-passing barriers (front running)
- ❑ Theft or loss of control (data)
- ❑ Third parties and vendors
- ❑ Supplier concentration



Program Maturity
- ❑ Culture of teamwork
- ❑ Governance framework
- ❑ Risk-based approach
- ❑ Industry frameworks
- ❑ Audits results
- ❑ Accredited benchmarking
- ❑ Time to respond
- ❑ Resiliency

Crown Jewels
- Investor Personal Data (PII)
- Fund Investments
- Fund Portfolio Construction
- Fund Trading Strategies
- Fund Financials & NAVs
- Research Notes
- Adviser Sensitive Data

Threat Actors
- ❑ Human flaws
- ❑ Hackers
- ❑ Cyber criminals
- ❑ Nation States

Vulnerabilities
- ❑ Software: WannaCry, NotPetya
- ❑ Technology: Spectre, Meltdown
- ❑ Facilities: physical data theft, tailgating
- ❑ Processes: control design blind spots
- ❑ Human: lack of understanding, malicious

Fund board oversight

- No federal statute or rule specifically requires a fund board to oversee risks, including cybersecurity risks.
  - SEC does require, however, that funds disclose the extent of the board's role in risk oversight.
- Risk oversight role derives from state law duty of care.
- Board practices for overseeing risk continue to evolve, and there is no uniform approach.

ICI/IDC Paper on Oversight of Risk Management

- Do not need to manage day-to-day fund operations.
- Board oversight includes:
  - understanding the risk management processes employed by the adviser,
  - asking questions where appropriate, and
  - obtaining appropriate assurances that the processes are reasonably designed to manage and control the fund's material risks.

Fund board oversight: SEC guidance and updates

- IM Guidance Update (April 2015)
  - Discusses a number of measures that funds and advisers may "wish to consider" when addressing cybersecurity risks.
- OCIE risk alerts
  - Summarize OCIE's findings following cybersecurity sweep exams (in 2014 – 2017).
- Speeches
  - Indicate heightened scrutiny on cybersecurity
- Statement and Guidance on Public Company Cybersecurity Disclosures (February 2018)
  - Stresses the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents.

Fund board oversight: recent developments

- OCIE 2018 Examination Priorities
  - Cybersecurity included as one of the exam priorities.
- SEC Enforcement Division Cyber Unit (created in September 2017)
  - Has identified failure by registered entities to take appropriate steps to safeguard information or ensure system integrity as an *enforcement interest.*
- Yahoo! Class Action
  - Based on materially false and misleading disclosures.

Fund board engagement: cybersecurity literacy

- Cybersecurity awareness is not cybersecurity literacy.
- How does board obtain cybersecurity literacy?
  - Understand the policies and procedures in place necessary to detect, respond to, and recover from cyberattacks.
  - Understand the legal implications of cybersecurity risks as they relate to fund company's particular circumstances.
  - Request tailored presentations from management, third-party service providers (transfer agent, fund accounting agent, custodian), and their IT professionals.
  - Stay abreast of SEC guidance, regulatory proceedings, litigation, and cyber incidents.
  - Attend educational programs and/or seek training from outside experts.

Fund board engagement: meeting protocol

- Establish a clear understanding with management that cybersecurity will be a key area of focus.
- Make cybersecurity a periodic board agenda item.
- Establish a reporting and notification policy.
  - Determine necessary frequency – should involve a risk assessment, but no less frequently than annually.
  - For non-routine issues, develop written policy detailing expectations.

Fund board engagement: ask questions and obtain assurances

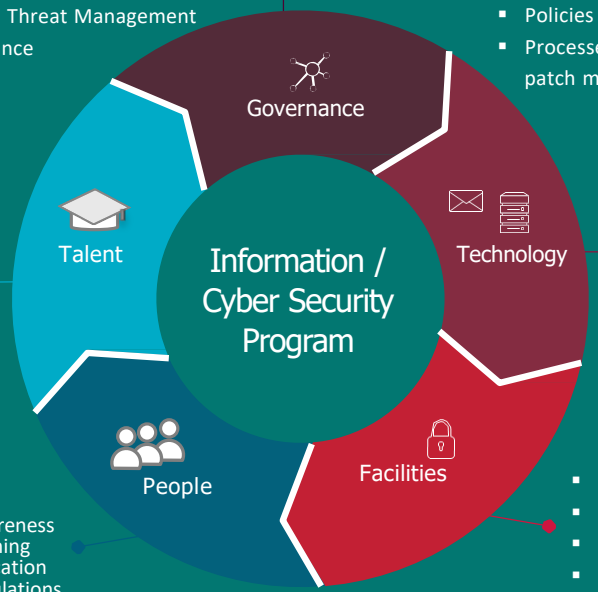
- Who is responsible for cybersecurity issues at management? Same person for third-party service providers? Is that person sufficiently knowledgeable about cybersecurity issues?
- What is the fund's critical data/information (*i.e.*, the "crown jewels")? Where is the data and who has access to it? Who is responsible for the data's security?
- If there is a data breach, who informs the responsible party? When is the board informed? Regulators, other authorities and/or shareholders?
- Is there mandatory employee training to deal with cybersecurity risks and, if so, how frequently is it given?
- What is the cybersecurity incident recovery process? Was it recently tested? How was it tested?
- Do disclosure documents include cybersecurity-specific disclosure and, if so, is the disclosure accurate in light of potential cybersecurity risks?

Fund board engagement: other considerations

- Understand contractual arrangements:
  - Distinction between new arrangements and existing.
  - Key provisions.
- Include detailed cybersecurity questions in questionnaires sent to advisers and service providers as part of the 15(c) process.
- Discuss and understand cyber-loss insurance.

Framework for board-adviser discussion

Program Influencers
- Laws and Regulations
- Industry best practices
- Technology pace of change
- Cyber threats
- Culture
- Firm's digital ecosystem
- Business practices
- Customers



- Oversight Committee
- Strategy
- Incident and Threat Management
- Cyber Insurance

- Risk Management
- Third-party Security Management (assessments, contract provisions)
- Policies (information / cyber security policy, acceptable use)
- Processes (data classification, security assurance, vulnerability and patch management)

- Identity, Access, Authentication and Entitlements
- Data protection (end-point encryption)
- Malware protection
- Spam filtering
- Phishing detection
- Application, system and network security baselines
- Encryption (data at-rest, in-motion)
- End-point (USB lockdown, local administrative rights)

- Badge access
- Turnstiles
- Cameras
- Security guards
- Environmental controls

- Awareness
- Training
- Education
- Simulations

- Workforce planning
- Skill development
- Career management

Resources for directors

- SEC IM Guidance Update, *Cybersecurity Guidance* (April 2015): https://www.sec.gov/investment/im-guidance-2015-02.pdf
- SEC Statement and Guidance on Public Company Disclosure (February 2018): https://www.sec.gov/rules/interp/2018/33-10459.pdf
- OCIE Risk Alerts
  - Observations from Cybersecurity Exams (August 2017): https://www.sec.gov/investment/im-guidance-2015-02.pdf
  - Cybersecurity Sweep Examination Summary (February 2015): https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf

Resources for directors

- SEC Speeches on Cybersecurity
  - Mary Jo White, former Chair of the SEC, The Fund Director in 2016: Keynote Address at the Mutual Fund Directors Forum 2016 Policy Conference: https://www.sec.gov/news/speech/chair-white-mutual-fund-directors-forum-3-29-16.html
  - Mary Jo White, former Chair of the SEC, Keynote Address Investment Company Institute 2016 General Meeting – "The Future of Investment Company Regulation: https://www.sec.gov/news/speech/white-speech-keynote-address-ici-052016.html
  - Stephanie Avakian, Co-Director, Division of Enforcement, The SEC Enforcement Division's Initiatives Regarding Retail Investor Protection and Cybersecurity: https://www.sec.gov/news/speech/speech-avakian-2017-10-26
- ICI Resource Center on Information Security: https://www.ici.org/info_security

Resources for directors

- CyberWire
  - https://thecyberwire.com/
- Data Breach Today
  - http://www.databreachtoday.com/
- Privacy Rights Clearinghouse
  - https://www.privacyrights.org/data-breaches
- Krebs on Security
  - https://krebsonsecurity.com/