Cyber Defense in Private Funds (Part 2)
A Talk with Michelle Reed

- Regulatory framework continued
  - Regulation S-P is intentionally broad, relying on industry to self-regulate. Diligence requires more than the minimum requirements of the law. The rules generally require some reasonable security measures, which would require firms to understand and respond to their specific risks.
  - States:
    - E.g. In 2017, New York Department of Financial Services (DFS) adopted expansive cybersecurity requirements for financial services companies,[1] including requirements for levels of encryption at rest and in transit and risk assessments, and requirements for vendors. NYCRR § 500.[2]
    - Does not apply to entities not regulated by the DFS, e.g. hedge funds, broker-dealers.
- Notice of breaches to regulators and affected individuals
  - States have varying notification requirements. Poses challenges for entities subject to multiple states' laws.
    - E.g. New York Shield Act amended New York's data breach notification laws to broaden the definition of "private information" and "breach" and imposing new data security requirements. "Breach" now includes unauthorized access—previously, included unauthorized acquisition only.
    - An important part of the incident response plan is how and when to communicate the breach to affected individuals. Some states require notification in 45 days or less of discovery.
    - DFS requires notification to the DFS within 72 hours of detection for certain cybersecurity events. GDPR also has a 72-hour requirement.
  - Futures
    - The CFTC issued an order against Phillip Capital Inc. (PCI), a registered futures commission merchant, for an email systems breach that resulted in cybercriminals withdrawing $1 million in customer funds.[3] Among other things, the order found that PCI failed to disclose to the breach to its customers in a timely manner and failed to supervise employees with respect to its cybersecurity policy and procedures. The order was the first time that the CFTC found that a

[1] New York State Department of Financial Services Cybersecurity Resource Center: https://www.dfs.ny.gov/industry_guidance/cybersecurity

[2] 23 NYCRR § 500. https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf

[3] CFTC Release Number 8008-19, CFTC Orders Registrant to Pay $1.5 Million for Violations Related to Cyber Breach: https://www.cftc.gov/PressRoom/PressReleases/8008-19

cybersecurity breach was "material information" giving rise to a disclosure obligation.

- Governance
  - Good governance requires effective incident response procedures, team, and tabletop exercises (breach exercises).
  - Quick tips for procedures and tabletop exercises
    - Run a risk assessment.
    - Assess the defenses.
    - Run a gap analysis in security.
    - Assess and address the gaps.
    - Assign a cybersecurity head inside the company. Don't task it to an unsupervised third party.
    - Conduct assessments and exercises annually.

- Risk of over-retention of data
  - The more data held and store, the higher the risk.
  - Every firm should have a data retention/destruction policy and ensure there is operational follow-through.
  - SEC requirement:
    - REG S-P: §248.30 Procedures to safeguard customer records and information; disposal of consumer report information:

      Proper disposal requirements: (2) *Proper disposal requirements*— (i) *Standard.* Every broker and dealer other than notice-registered broker-dealers, every investment company, and every investment adviser and transfer agent registered with the Commission, that maintains or otherwise possesses consumer report information for a business purpose must properly dispose of the information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.[4]

- California CCPA
  - The California Consumer Privacy Act (CCPA)[5] goes into effect January 2020. Generally, the CCPA provides that consumers have a right to know what information is collected and for what purposes and the right to access that information, and request that it be deleted or to opt out of it being sold to third parties.

[4] 65 FR 40362, June 29, 2000, as amended at 69 FR 71329, Dec. 8, 2004. https://www.ecfr.gov/cgi-bin/text-idx?node=17:4.0.1.1.8&rgn=div5#se17.4.248_130
[5] California Consumer Privacy Act (CCPA): https://oag.ca.gov/privacy/ccpa

- Best practices
  - SEC's 2015 Cybersecurity Guidance[6]:
    - The OCIE published the results of examinations to assess the steps investment advisers are taking to address cybersecurity.
      - Conduct periodic assessments of the information the firm collects, cybersecurity threats and vulnerabilities, current controls in place, the impact of a breach, and the effectiveness of the governance structure.
      - Create a strategy to prevent, detect and respond to threats, including data encryption, data backup, and incident response plans.
      - Implement written policies and procedures and train employees.
  - Engaging with 3rd parties
    - Conduct due diligence. Review vendor cybersecurity policies.
    - Background checks and confidentiality agreements with new hires.
    - Contract for responsibility for data security and privacy compliance, indemnification, and cyber insurance.

[6] SEC Cybersecurity Guidance https://www.sec.gov/investment/im-guidance-2015-02.pdf