Cyber Defense in Private Funds (Part 1)
A Talk with Michelle Reed

- As firms are implementing more technology into their activities, their risks are multiplying. The private funds industry is a particularly high value target because they conduct large transactions and hold highly sensitive information on investors, investment targets, and others. In the digital world, a cybersecurity breach is a matter of "when," not "if."
    - Because most funds lack the resources and manpower of large banks, cybersecurity is often an afterthought. But with increasing threats, the best line of defense is to prepare prior to any attacks. Good governance is essential to guard against the constantly changing threats.
    - Risks and vulnerabilities
        - Funds are treasure troves of data. They may hold sensitive data on the management company, employees, limited partners, portfolio companies, investment targets, and third party vendors.
        - Risks include business disruption; poaching of IP, trade secrets, or other valuable data; destruction or public disclosure of private data, conversion of funds; business disruption; reputational harm; and legal liability.

- Attack methods
    - Phishing
        - One of the most common methods. Usually in the form of an email purported to be from a reputable or trusted source and contains a link designed to steal information or convert funds.
        - Spear phishing involves a more targeted and specific attack; often, the cybercriminals will impersonate company insiders or known vendors.
        - Cybercriminals employ social engineering schemes to encourage recipient to click on a link, download files, transfer funds, etc.
        - SEC21(a) report[1]
            - Though the below investigation involved public companies, it indicates increased regulatory and enforcement focus across all sectors and businesses.
            - The SEC investigated 9 public companies on "business email compromises" though it did not pursue enforcement actions. The 9 companies lost a total of nearly $100 million as a result of the compromises. "Business email compromises" included

[1] Securities and Exchange Commission, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements, Release No. 84429, October 16, 2018. https://www.sec.gov/litigation/investreport/34-84429.pdf

phishing attacks spoofing emails from company executives or vendors. The SEC advised that public companies should design controls that reasonably protect against cyber-attacks.
        - The 21(a) report indicates that the SEC will likely pursue enforcement actions against public companies for insufficient procedures in the future.
    - As a first level defense, set up 2-factor authentications for emails.
- Advanced persistent threats (APT)
    - APT uses sophisticated methods to capitalize on vulnerabilities in a system and gain access. The threat remains in the system for an extended period of time, often lying in wait. It may create a network of backchannels that allows it to move around the system freely between servers.
    - APT is typically perpetrated by governments or sophisticated criminal organizations and against other states or large corporations.
- Ransomware
    - Type of malware that encrypts files or locks a user out of their computer until a ransom is paid in exchange for the decryption key. Ransomware can migrate from one infected computer or system to another. Commonly delivered though emailed links or attachments. Ransomware may also be a cover for more advanced threats.
    - In the case of a ransomware attack, the two choices typically are restoring a backup or paying the ransom.
        - To ensure any potential ransomware attacks do not affect the backup, the disaster recovery backup should be stored sufficiently separate from the rest of the system.
        - Paying the ransom
            - When there is no backup or restoring a backup is not feasible, it may be the only option. Many firms, as a result, take on cyber security policies that also cover ransomware attacks.
            - Paying the ransom is generally not prohibited under U.S. law. However, the U.S. prohibits conducting financial transactions with parties listed on Sanctions Lists. [2] Maintained by the Treasury Department's Office of Foreign Assets Control (OFAC), the Sanctions List includes foreign governments, terror groups, and individuals. Trading with the Enemy Act prohibits providing support to any entity on the sanctions lists. The

[2] Department of the Treasury Office of Foreign Assets Control – Sanctions Programs and Information: https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx

fines and penalties may vary depending on the statutory authority for the sanction.[3]

- Registered investment advisers regulated by the SEC
    - SEC's Office of Compliance Inspections and Examinations (OCIE) conducts examinations to ensure regulatory compliance, inform policy, and monitor risk. OCIE exam priorities in the past 5-7 years have consistently included cybersecurity.
    - In the past, the OCIE's exam requests were largely based the National Institute of Standards and Technology (NIST) framework, which outlines guidance for organization to create infrastructure to detect and respond to cyberthreats.[4] Its focus was mainly on assessing cybersecurity preparedness. In recent years, OCIE exam requests indicate that data privacy is a key concern, ensuring compliance with existing data privacy laws like REG S-P and REG S-ID.
        - Regulation S-P: requires registered advisers to adopt written policies to safeguard customer information.[5]
        - Regulation S-ID: requires registered advisers to adopt written a written identity theft prevent program that, among other things, identify red flags, regularly monitor accounts, and is periodically updated based on risk changes.[6]

[3] *See* 31 C.F.R. Part 578 – Cyber-Related Sanctions Regulations: https://www.govinfo.gov/app/details/CFR-2016-title31-vol3/CFR-2016-title31-vol3-part578/summary
[4] NIST Cybersecurity Framework: https://www.nist.gov/cyberframework
[5] Regulation S-P: https://www.sec.gov/spotlight/regulation-s-p.htm
[6] Regulation S-ID: https://www.sec.gov/rules/final/2013/34-69359.pdf