RISK ALERT
OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS

July 10, 2020

# CYBERSECURITY: RANSOMWARE ALERT

The Office of Compliance Inspections and Examinations (OCIE)* is committed to working with financial services market participants, federal, state and local authorities, and others, to monitor cybersecurity developments, improve operational resiliency, and effectively respond to cyber threats. Recent reports indicate that one or more threat actors have orchestrated phishing and other campaigns designed to penetrate financial institution networks to, among other objectives, access internal resources and deploy ransomware. Ransomware is a type of malware designed to provide an unauthorized actor access to institutions' systems and to deny the institutions use of those systems until a ransom is paid.

OCIE has also observed an apparent increase in sophistication of ransomware attacks on SEC registrants, which include broker-dealers, investment advisers, and investment companies. The perpetrators behind these attacks typically demand compensation (ransom) to maintain the integrity and/or confidentiality of customer data or for the return of control over registrant systems. In addition, OCIE has observed ransomware attacks impacting service providers to registrants.

In light of these threats, OCIE encourages registrants, as well as other financial services market participants, to monitor the cybersecurity alerts published by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), including the updated alert published on June 30, 2020 relating to recent ransomware attacks.[1] OCIE further encourages registrants to share this information with their third-party service providers, particularly with those that maintain client assets and records for registrants.

***CISA Alert – Dridex Malware*** available at https://www.us-cert.gov/ncas/alerts/aa19-339a

---

* The views expressed herein are those of the staff of OCIE. This Risk Alert is not a rule, regulation, or statement of the Securities and Exchange Commission (the SEC or the Commission). The Commission has neither approved nor disapproved the content of this Risk Alert. This Risk Alert has no legal force or effect: it does not alter or amend applicable law, and it creates no new or additional obligations for any person. This document was prepared by OCIE staff and is not legal advice.

[1] CISA is responsible for protecting the Nation's critical infrastructure from physical and cyber threats. This mission requires effective coordination and collaboration among a broad spectrum of government and private sector organizations. (www.cisa.gov)

The CISA alert referenced above highlights tactics and techniques used by certain threat actors, along with related indicators of compromise (IOCs) and key mitigation strategies to reduce overall vulnerability.

Recognizing that there is no such thing as a "one-size fits all" approach, and that not all of these practices may be appropriate for every organization, we are also providing the following observations to assist market participants in their consideration of how to enhance cybersecurity preparedness and operational resiliency to address ransomware attacks.[2] We have observed registrants utilizing the following measures:[3]

- ***Incident response and resiliency policies, procedures and plans.*** Assessing, testing, and periodically updating incident response and resiliency policies and procedures, such as contingency and disaster recovery plans. These policies and procedures may include, for example:
    - Response plans for various scenarios, including, among others, ransomware and other denial of service attacks.
    - Procedures for the timely notification and response if an event occurs, a process to escalate incidents to appropriate levels of management (including legal and compliance functions), and communication with the registrant's key stakeholders.
    - Procedures for addressing compliance with federal and state reporting requirements for cyber incidents or events, such as financial institution suspicious activity report filing requirements or reporting of material events under the federal securities laws.
    - Procedures to contact law enforcement, inform regulators and promptly notify new and existing customers and clients, as appropriate.
- ***Operational resiliency.*** Determining which systems and processes are capable of being restored during a disruption so that business services can continue to be delivered.
    - Focusing on a capability to continue to operate critical applications in the event that the primary system is unavailable.

---

[2] Additional ransomware "cyber defense best practices" can be found at FBI Public Services Announcement – High Impact Ransomware Attacks Threaten U.S. Businesses and Organizations. (https://www.ic3.gov/media/2019/191002.aspx)

[3] A number of these measures are also described in our January 27, 2020 report on Cybersecurity and Resiliency Observations, available at https://www.sec.gov/files/OCIE-Cybersecurity-and-Resiliency-Observations-2020-508.pdf.

- Ensuring geographic separation of back-up data and writing back-up data to an immutable storage system in the event primary data sources are unavailable.

- ***Awareness and training programs.*** Providing specific cybersecurity and resiliency training, and considering undertaking phishing exercises to help employees identify phishing emails. Training provides employees with information concerning cyber risks and responsibilities and heightens awareness of cyber threats such as ransomware.

- ***Vulnerability scanning and patch management.*** Implementing proactive vulnerability and patch management programs that take into consideration current risks to the technology environment, and that are conducted frequently and consistently across the technology environment.

    - Ensuring all firmware, operating systems and application software (*i.e.,* in-house developed, custom off-the-shelf, and other third-party software), and anti-virus and other host-based security tools have the most current updates.

    - Ensuring anti-virus and anti-malware solutions are set to update automatically and that regular scans are conducted, and considering upgrading anti-malware capability to include advanced endpoint detection and response capabilities.

- ***Access management.*** Managing user access through systems and procedures that: (i) limit access as appropriate, including during onboarding, transfers, and terminations; (ii) implement separation of duties for user access approvals; (iii) re-certify users' access rights on a periodic basis (paying particular attention to accounts with elevated privileges including users, administrators, and service accounts); (iv) require the use of strong, and periodically changed, passwords; (v) utilize multi-factor authentication leveraging an application or key fob to generate an additional verification code; and (vi) revoke system access immediately for individuals no longer employed by the organization, including former contractors. Configuring access controls so users operate with only those privileges necessary to accomplish their tasks (*i.e.,* least privilege access).

- ***Perimeter security.*** Implementing perimeter security capabilities that are able to control, monitor, and inspect all incoming and outgoing network traffic to prevent unauthorized or harmful traffic. These capabilities include firewalls, intrusion detection systems, email security capabilities, and web proxy systems with content filtering.

    - Employing best practices for use of Remote Desktop Protocol (RDP), including auditing networks for systems using RDP, closing unused RDP ports, and monitoring RDP login attempts. Exposing RDP to the Internet is a significant vulnerability and risk, which can be addressed by supporting RDP only through an encrypted Virtual Private Network connection.

- Using an application control capability that ensures only approved software can be executed.
- Using a security proxy server to control and monitor access to the Internet to address potential security vulnerabilities of Internet connections.

The SEC has focused on cybersecurity issues for many years, with particular attention to market systems, customer data protection, disclosure of material cybersecurity risks and incidents, and compliance with legal and regulatory obligations under the federal securities laws. Among other resources, the SEC maintains a Cybersecurity Spotlight webpage that provides cybersecurity-related information and guidance.[4] Cybersecurity has been a key examination priority for OCIE for many years, identifying information security as a key risk area on which registrants should focus. In addition to the Cybersecurity and Resiliency Observations Report noted above, OCIE has also published several additional cybersecurity-related risk alerts.[5]

*This Risk Alert is intended to highlight for firms risks and issues that OCIE staff has identified. In addition, this Risk Alert describes risks that firms may consider to (i) assess their supervisory, compliance, and/or other risk management systems related to these risks, and (ii) make any changes, as may be appropriate, to address or strengthen such systems. Other risks besides those described in this Risk Alert may be appropriate to consider, and some issues discussed in this Risk Alert may not be relevant to a particular firm's business. The adequacy of supervisory, compliance and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.*

4 "Spotlight on Cybersecurity, the SEC and You" available at www.sec.gov/spotlight/cybersecurity. This page contains information for investors, issuers, and registered firms and organizations, including the Commission Statement and Guidance on Public Company Cybersecurity Disclosures, guidance from the Division of Investment Management, the Division of Trading and Markets, and Investor Alerts and Bulletins.

5 Additional OCIE Risk Alerts that address cybersecurity and other examination issues are available at www.sec.gov/ocie.