WINSTON & STRAWN LLP

CLIENT ALERT

OCIE Warns of Increasingly Sophisticated Ransomware Attacks Affecting SEC Registrants

JULY 17, 2020

On July 10, 2020, the U.S. Securities and Exchange Commission (SEC) Office of Compliance Inspections and Examinations (OCIE) released a Risk Alert (OCIE Alert) warning SEC registrants about the observed apparent increase in the sophistication of cybersecurity attacks on SEC registrants including broker-dealers, investment advisers, and investment companies.[1] These attacks have also impacted third-party service providers to SEC registrants.

OCIE reports that bad actors have been orchestrating phishing campaigns and other cybersecurity attacks designed to penetrate the networks of financial institutions to gain access to internal resources and deploy ransomware, among other objectives. Ransomware is a type of malware designed to prevent authorized users from accessing an institution's systems while the perpetrators demand compensation (a ransom) to maintain the integrity and/or confidentiality of the affected data or to return control over the systems to the institution.

OCIE encourages SEC registrants and other financial services market participants to familiarize themselves with the risks of ransomware attacks and to prepare their internal systems to avoid and mitigate attacks. OCIE encourages market participants to monitor the cybersecurity alerts published by the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA),[2] particularly the newly updated alert CISA released on June 30 addressing recent ransomware attacks (CISA Alert).[3] OCIE also encourages registrants to share this information with their third-party service providers that may be impacted by ransomware attacks, particularly service providers that maintain confidential client information for registrants such as client assets and records.

The OCIE Alert emphasizes the importance of the CISA Alert's discussion of tactics and techniques used by bad actors in certain cybersecurity attacks and highlights certain strategies to mitigate the risk of these tactics and reduce the overall vulnerability of market participants to such attacks. While the OCIE Alert recognizes that there is no "one size fits all" approach that will work for every organization, OCIE provides several examples of measures that market participants have used to help enhance cybersecurity preparedness and operational resiliency to prevent and address potential ransomware attacks. In particular, OCIE has observed SEC registrants using measures including the following:

Incident response and resiliency policies, procedures, and plans. Market participants may assess, test, and periodically update their incident response and resiliency policies and procedures, including contingency and disaster recovery plans. These policies and procedures may include response plans for potential disruption scenarios such as ransomware attacks, procedures to respond to attacks and timely notify internal and external stakeholders, compliance with cybersecurity incident reporting requirements, and procedures to contact law enforcement, inform regulators, and/or notify customers and clients, as appropriate.

Operational resiliency. SEC registrants may formulate plans to restore systems and processes during a disruption event so the institution may continue to provide business services. These plans may include a focus on the capability to continue to operate critical applications in the event that access to the primary system is disrupted and ensuring back-up data is stored separately from the primary data sources in the event the primary systems become unavailable.

Awareness and training programs. Institutions may provide specific cybersecurity and resiliency training to their personnel to provide employees with information concerning cybersecurity risks and responsibilities and make employees aware of cybersecurity threats such as ransomware. Institutions may also consider measures such as undertaking phishing exercises to help employees identify and appropriately respond to phishing emails.

Vulnerability scanning and patch management. SEC registrants may implement proactive vulnerability and patch management programs to ensure all institutional systems are up-to-date. This may include setting up antivirus and antimalware software to update automatically and upgrading antimalware capabilities to include advanced endpoint detection and response capabilities.

Access management. Market participants manage user access through various systems and procedures including policies designed to limit access as appropriate, requiring users to periodically recertify access, requiring the use of strong and periodically changed passwords, using multi-factor authentication, immediately revoking system access for individuals who no longer work with the organization (including former employees and contractors), and configuring system access so users only have access to the functions necessary to accomplish their tasks (least privilege access).

Perimeter security. Institutions may implement perimeter security capabilities to control, monitor, and inspect all incoming and outgoing network traffic. This allows institutions to prevent unauthorized and harmful traffic. These capabilities include measures such as firewalls, intrusion detection systems, email security capabilities, and web proxy systems with content filtering. For example, institutions may monitor and limit remote access to systems, such as by allowing remote desktop access only through the use of an encrypted Virtual Private Network connection.

The SEC maintains a public website to provide cybersecurity-related information and guidance for investors, issuers, and registered firms and organizations.[4] OCIE has also focused on cybersecurity risks, including publishing a report on "Cybersecurity and Resiliency Observations."[5]

[1] Cybersecurity: Ransomware Alert (July 10, 2020).

[2] CISA publishes these alerts to its website.

[3] Dridex Malware, Alert (AA19-339A) (rev. June 30, 2020).

[4] Spotlight on Cybersecurity, the SEC, and You.

[5] Cybersecurity and Resiliency Observations. Additional OCIE risk alerts, including various alerts focused on cybersecurity issues, may be found on the OCIE website.

4 Min Read

Related Locations

Charlotte | Chicago | Dallas | Houston | Los Angeles | New York | San Francisco | Silicon Valley | Washington, DC

Related Topics

Corporate | Investment Management | Securities and Exchange Commission (SEC) | Office of Compliance Inspections and Examinations

Related Capabilities

Transactions | Private Investment Funds

Related Regions

North America

Related Professionals

Michael Wu