OCIE Ransomware Alert: Stay Alert, Stay Prepared

July 14, 2020

AUTHORS

Daniel K. Alvarez | Elizabeth P. Gray | Elizabeth Bower | Richard M. Borden

On July 10, 2020, the SEC's Office of Compliance Inspections and Examinations ("OCIE") released a Risk Alert (the "OCIE Alert") focused on the increasing threat to financial firms posed by sophisticated ransomware attacks on SEC registrants, including broker-dealers, investment advisers, and investment companies, and also ransomware attacks impacting service providers to registrants. Specifically, OCIE stated that "[r]ecent 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."

As we discussed with our colleague from KPMG in a recent webinar, "Ransomware: Knowing and Managing Your Regulatory Obligations," the technology and strategy driving ransomware has been evolving. What once was a blunt, anonymous attack designed to encrypt your data and hold it for ransom has become a targeted effort to leverage the threat actor's access to the data to hold the victim hostage. This was confirmed in the OCIE Alert, where it says that it has "observed an apparent increase in sophistication of ransomware attacks" and notes that these attacks are targeting both "SEC registrants, which include broker-dealers, investment advisers, and investment companies" and their service providers.

Staying Alert and Staying Prepared

In light of these threats, the OCIE Alert highlights two key pillars of any cyber-defense strategy: staying alert, and staying prepared. As to the former, the Alert "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)." The alert specifically highlights a CISA Alert published on June 30, 2020 relating to recent

ransomware attacks that employ a new variant of ransomware increasingly used by threat actors. The CISA Alert provides information about how threat actors are using this new malware, the "indicators of compromise" associated with the malware, and key mitigation strategies.[1] Financial firms are encouraged to share this CISA Alert with their partners and service providers, to ensure the information is as widely distributed as possible.

With respect to staying prepared, the OCIE Alert highlights many of the strategies and practices that OCIE has observed in the course of conducting its investigations and examinations of financial firms, while recognizing that "there is no such thing as a "one-size fits all" approach." These include:

- ***Robust incident response and resiliency policies, procedures and plans.*** The OCIE Alert explicitly highlights the importance of assessing, testing, and periodically updating incident response and resiliency policies and procedures, including by testing the plans against scenarios like a successful ransomware attack.

- ***Operational resiliency.*** The OCIE Alert reinforced the importance of taking steps to ensure that critical applications can continue to operate during an incident, such as by geographically separating back-up data from production data, and having a plan in place to identify and restore systems to minimize downtime. This is one of the most important and difficult issues to address in the context of ransomware, as data may be available offline, but if systems and networks are not the impact may be severe. From a resiliency standpoint, planning and preparedness should address the possibility that other protections will fail.

- ***Awareness and training programs.*** The OCIE Alert emphasized the role of specific cybersecurity and resiliency training, including phishing exercises that help employees better 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.*** Vulnerability and patch management programs should be conducted regularly, and should be sufficiently flexible to account for changes to technology, tactics, and strategies employed by threat actors. At a minimum, it is important to ensure that all firmware, operating systems and application software, and anti-virus and other security tools are properly updated.

- ***Access management.*** Because many threat actors infiltrate networks by hijacking legitimate accounts through phishing emails and other similar tactics, configuring your network's access controls so that users operate with only those privileges necessary to accomplish their tasks is a critical component of any cyber-defense strategy. Other key components of access management strategies highlighted by the OCIE Alert include re-certifying users' access rights on a periodic basis, utilizing multi-factor authentication, leveraging an application or key fob to

[1] CISA Alert – Dridex Malware available here.

generate an additional verification codes, and revoking system access immediately for individuals no longer employed by the organization, including former contractors.

- ***Perimeter security.*** Perimeter security capabilities should be able to control, monitor, and inspect all incoming and outgoing network traffic to prevent unauthorized or harmful traffic. Firewalls, intrusion detection systems, and web proxy systems with content filtering will be important components of this effort.

Moving Forward

As we have highlighted in previous alerts, the COVID-19 pandemic has changed the way we work and interact in numerous ways that increase the risk of cyber-based attacks to our networks and IT infrastructure. The Department of Homeland Security, Federal Trade Commission, and numerous other federal and state agencies have highlighted the increasing prevalence of cyber and other frauds that leverage the pandemic. This OCIE Alert reinforces the need to adopt some of these key strategies to protect your data and IT infrastructure and adapt them to your company's specific risk profile.

Willkie has multidisciplinary teams working with clients to address coronavirus-related matters, including, for example, contractual analysis, litigation, restructuring, financing, employee benefits, SEC and other corporate-related matters, and CFTC and bank regulation. Please click here to access our publications addressing issues raised by the coronavirus. For advice regarding the coronavirus, please do not hesitate to reach out to your primary Willkie contacts.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Elizabeth P. Gray
202 303 1207
egray@willkie.com

Elizabeth Bower
202 303 1252
ebower@willkie.com

Richard M. Borden
212 728 3872
rborden@willkie.com