Published on *The National Law Review* https://natlawreview.com

OCIE Issues Ransomware Risk Alert

Article By:

John S. Marten

Nathaniel Segal

Jacob C. Tiedt

Kelly Pendergast Carr

Responding to an apparent increase in sophistication of ransomware attacks on SEC registrants, and attacks impacting registrants' service providers, the SEC's Office of Compliance Inspections and Examinations (OCIE) issued a risk alert on July 10, 2020 encouraging market participants to consider enhancements to cybersecurity preparedness and operational resiliency to address these attacks. OCIE cited the importance of assessing, testing and periodically updating incident response and resiliency policies and procedures, such as contingency and disaster recovery plans, in maintaining operational resiliency. OCIE also suggested measures such as:

- awareness and training programs, including phishing exercises;
- programs to ensure all firmware, operating systems and other applications are updated and have the appropriate anti-virus and anti-malware solutions;
- policies and procedures to limit access and controls so users operate with only those privileges necessary to accomplish their tasks (i.e., least privilege access); and
- implementing perimeter security capabilities, such as firewalls, intrusion detection systems, email security capabilities and web proxy systems with content filtering.

In addition to the foregoing, OCIE encouraged registrants to monitor the cybersecurity alerts published by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA). CISA Alerts are available here.

You can read the full risk alert here.

National Law Review, Volume X, Number 220