CRAVATH, SWAINE & MOORE LLP

David M. Stuart
+1-212-474-1519
dstuart@cravath.com

Evan Norris
+1-212-474-1524
enorris@cravath.com

John W. White
+1-212-474-1732
jwhite@cravath.com

David Greenwald
+1-212-474-1922
dgreenwald@cravath.com

Rachel G. Skaistis
+1-212-474-1934
rskaistis@cravath.com

John D. Buretta
+1-212-474-1260
jburetta@cravath.com

Benjamin Gruenstein
+1-212-474-1080
bgruenstein@cravath.com

U.S. Securities and Exchange Commission Issues Report on Cybersecurity and Resiliency Practices

January 29, 2020

On January 27, 2020, the U.S. Securities and Exchange Commission released a report reflecting its latest observations on cybersecurity and resiliency practices. This report once again highlights that the SEC is paying special attention to cybersecurity issues as they relate to market systems, disclosure of material risks and incidents, customer data protection and compliance.[1] While the SEC unit that issued the report—the Office of Compliance Inspections and Examinations ("OCIE")—is responsible for examinations of regulated entities such as broker-dealers, investment advisers and investment companies, the observations are applicable to public companies across a range of industries at a time when cybersecurity threats continue to touch every region of the world and virtually every sector of the economy.

The report addresses the following cybersecurity risks and explains how organizations have managed and mitigated them:

- Governance and risk management—establishing board and senior leadership oversight of cybersecurity and resiliency programs, conducting risk assessments, creating written policies and procedures that address cybersecurity issues, testing and monitoring of relevant policies, updating policies and procedures to address any gaps or weaknesses and developing methods of communicating internally and externally regarding cybersecurity issues.

- Access rights and controls—understanding, managing and monitoring user access to data and systems.

- Data loss prevention—developing a vulnerability management program to conduct routine scans, implementing security measures to intercept threats and block access to personal email or other insecure platforms, implementing security measures to detect threats at endpoints, using a patch management program, keeping an inventory of hardware and software assets, using encryption and network segmentation, monitoring insider threats and securing legacy systems and equipment.

[1] See our client alerts "U.S. Securities and Exchange Commission 2019 Budget Request Prioritizes Cybersecurity Enforcement and Management of Internal Cybersecurity Risk" (Feb. 14, 2018), https://www.cravath.com/US-SEC-2019-Budget-Request-Prioritizes-Cybersecurity-Enforcement-and-Management-of-Internal-Cybersecurity-Risk-02-16-2018/; and "U.S. Securities and Exchange Commission Cautions Public Companies on Risks Arising from Cyber-Related Frauds" (Oct. 24, 2018), https://www.cravath.com/US-Securities-and-Exchange-Commission-Cautions-Public-Companies-on-Risks-Arising-from-CyberRelated-Frauds-10-26-2018/.

- Mobile security—creating policies and procedures relating to the use of mobile devices, managing use of mobile devices, mandating the use of multi-factor authentication and training employees on relevant policies and procedures.

- Incident response—establishing a risk-assessed incident response protocol, complying with applicable state and federal reporting requirements, designating responsibilities for specific employees in the event of a cyber-related incident and testing the incident response protocol.

- Resiliency—keeping inventory of core business systems and processes, creating an operational resiliency strategy that assesses risk tolerance and contemplating other safeguards such as storing back-up data offline or on another network.

- Vendor management—establishing a vendor management program to ensure that security measures and other safeguards are followed, understanding the specific terms of any agreements with vendors and monitoring and testing the vendor relationship for potential issues.

- Training and awareness—training employees on cybersecurity policies and procedures, providing employees with specific examples and exercises during training and monitoring the effectiveness of training.

The report concludes by encouraging companies to review their policies, practices and procedures with respect to cybersecurity preparedness and operational resiliency.

At a time when the SEC and other U.S. enforcement authorities are focused on compliance, governance and risk management programs in the context of corporate investigations—and willing to provide credit for sound programs—we encourage clients to prioritize conducting and documenting a cybersecurity risk assessment as part of their regular compliance risk assessment. We believe this is likely to continue to be a significant focus of U.S. enforcement authorities in the near term.

This publication, which we believe may be of interest to our clients and friends of the firm, is for general information only. It should not be relied upon as legal advice as facts and circumstances may vary. The sharing of this information will not establish a client relationship with the recipient unless Cravath is or has been formally engaged to provide legal services.

New York
Worldwide Plaza
825 Eighth Avenue
New York, NY 10019-7475
+1-212-474-1000

London
CityPoint
One Ropemaker Street
London EC2Y 9HR
+44-20-7453-1000

www.cravath.com