BCLP. Client Intelligent

Insights

NY DFS CYBERSECURITY SYMPOSIUM: MORE RIGOROUS RULES, EXAMS AND ENFORCEMENT AHEAD

Apr 05, 2022

The New York Department of Financial Services ("DFS") is turning up the heat on cybersecurity once again. During its first-ever Cybersecurity Symposium on March 29, DFS announced a series of new measures that will require regulated entities to bolster their cybersecurity controls and give DFS additional tools to monitor compliance. DFS was a trailblazer when it first adopted the Cybersecurity Regulation in 2017, and these changes reaffirm its role as a leading regulator in the cybersecurity space.

The Symposium featured presentations by Executive Deputy Superintendent, Justin Herring, who announced upcoming changes to the Cybersecurity Regulation, and Assistant Deputy Superintendent, William Peterson, who outlined the new Part 500 Examinations process. A summary of the upcoming changes appears below.

The overarching message from DFS, however, was clear: cybersecurity remains a key priority and regulated entities should be prepared for more rigorous scrutiny of their cybersecurity practices across all levels of their organizations, particularly at the top.

Amendments to the Cybersecurity Regulation

DFS first announced that it was considering changes to the Cybersecurity Regulation in June 2021, and, according to Mr. Herring, work on those changes is ongoing. Although Mr. Herring declined to provide details, he said the updated rules will retain the same overall risk-based framework that appears in the existing Regulation and continue to focus on the need for comprehensive risk assessments and adequate cybersecurity policies and procedures.

Notable changes, however, can be expected in several other areas. According to Mr. Herring, DFS is looking to include "more specifics" around the need to protect remote access and conduct an asset inventory. Additional details also are being considered on the topic of governance and will focus on the oversight role of the Board and C-Suite. DFS is also considering "clarifying" its incident reporting requirements particularly with respect to ransomware and situations involving access to privileged accounts.

In addition, an expanded list of “minimum controls” – beyond encryption and multifactor authentication – can be expected. According to Mr. Herring, some insight into the additional controls may be gleaned from recent DFS Guidance on Ransomware, Multifactor Authentication and the Ukraine. A review of that Guidance suggests that these additional controls may include the following:

Additional Controls Identified in Recent NY DFS Guidance
Email Filtering and Anti-Phishing Training
Vulnerability & Patch Management with Periodic Penetration Testing
Multifactor Authentication for Remote Access and External/Third Party Apps
Disabling Remote Desktop Protocol Access
Password Management
Privileged Access Management
Network Segmentation
Endpoint Detection Monitoring and Response
Maintaining and Testing Segregated Backups
Incident Response Plans that Explicitly Address Ransomware

DFS did not provide a timeline for its release of these new rules, but promised that they would be subject to a notice and comment period prior to being finalized.

New Standards and Tools for Compliance

DFS also announced efforts to “modernize” its supervision process by heightening attention on cybersecurity issues. According to Mr. Peterson, the DFS Part 500 exams currently focus on three areas: (1) prior examination data, which includes any Part 500 violations; (2) annual certification status; and (3) cybersecurity events, whether reported or not, and any significant business continuity issues.

Going forward, DFS will be using two new tools to help it assess the strength of an entity’s cybersecurity program. One tool will be the “Cybersecurity and Information Technology Baseline Risk Questionnaire” (“CIBRQ”) which DFS expects to begin using in 2023. The CIBRQ is an online questionnaire that regulated entities will be required to complete and periodically update. According to DFS, it will cover the following 11 topics:

CIBRQ Topics	
Independent Audit	Endpoint Detection
Organization Structure	Vulnerability/Patch Mgmt.
Awareness Training	Monitoring/Detection
Third Party	Incident Response
Asset Management	Business Continuity
Authentication	

The other new tool DFS will be using to assess cybersecurity risk is SecurityScorecard. SecurityScorecard collects open source information to compile a cybersecurity rating for a company. The rating is based on an analysis of this publicly available data across a number of different factors, including the following eight factors identified by DFS:

SecurityScorecard Factors for DFS	
Network Security	Application Security
DNS Health	Hacker Chatter
Patching Cadence	Information Leak
IP Reputation	Social Engineering

DFS is also investing in its own operations by hiring additional personnel and training examiners on cybersecurity developments and related DFS guidance.

Take-Away

During the upcoming months, regulated entities should confirm that they have updated risk assessments and adequate policies and procedures in place. They also should take steps to ensure that they have implemented, or have a plan to implement, the specific controls outlined in DFS Guidance, and are prepared to answer questions regarding the CIBRQ topics and address any deficiencies reflected in their SecurityScorecard ratings.

Up Next: Governance Issues with Keynote by Superintendent Adrienne Harris

The Cybersecurity Symposium on March 29 was the first of three programs DFS has scheduled for the upcoming months. The next program, being held on April 26, 2022, will focus on governance and is entitled “The Human Factor: Leadership, Governance and Diversity in Cybersecurity.” This program will feature a keynote address by the newly appointed DFS Superintendent, Adrienne Harris.

The third program, scheduled for May 24, 2022, will address cybersecurity issues for small and mid-sized businesses. This program is entitled “Spotlight on Small Business: DFS and Global Cybersecurity Alliance Share Achievable Cybersecurity Controls for Smaller Organizations.”

Additional information about these upcoming programs and access links may be found on the DFS website or by clicking here.

RELATED PRACTICE AREAS

- Data Privacy & Security
- Financial Regulation Compliance & Investigations
- Insurance
- Litigation & Dispute Resolution
