Hogan Lovells

A guide to NYDFS Cybersecurity Regulation's March 1 implementation deadline

February 28, 2018

It's been almost a year since the New York State Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR Part 500) came into effect (see our discussion here). Since that time, a series of key dates have marked the implementation of various portions of the regulations, starting with the August 28, 2017 deadline. Now, as we approach the one-year anniversary of the effective date of the Cybersecurity Regulation, another deadline looms. March 1, 2018 will mark the end of the one-year transitional period, at which time covered entities are required to be in compliance with additional requirements covering the following:

- Chief Information Security Officer (CISO) reporting to your board of directors
- penetration testing and vulnerability assessments
- risk assessments of your information systems
- multi-factor authentication or other effective controls
- cybersecurity awareness training for your personnel

As you finalize your organization's preparations for compliance, we have highlighted below key aspects of the portions of the Cybersecurity Regulation coming into effect on March 1: Sections 500.04(b), 500.05, 500.09, 500.12, and 500.14(b). In addition to this overview, you may also find the NYDFS's Frequently Asked Questions—which have been updated several times, most recently on February 23, 2018—a helpful resource in your preparation for this next implementation deadline.

Initial CISO Report (Section 500.04(b))

Under the Cybersecurity Regulation, the CISO must report in writing to your board of directors on your organization's cybersecurity program and material cybersecurity risks. If your organization does not have a board, the CISO must report to the equivalent governing body, or in the absence thereof, to a senior officer responsible for your cybersecurity program. Note that a report to a board subcommittee is not sufficient to meet the requirements under Section 500.04(b).

The CISO Report must provide information on the following, to the extent applicable:

- the confidentiality of nonpublic information and the integrity and security of your information systems
- cybersecurity policies and procedures
- material cybersecurity risks
- overall effectiveness of the cybersecurity program
- material cybersecurity events during the time period addressed by the report

Penetration Testing and Vulnerability Assessments (Section 500.05)

Under the Cybersecurity Regulation, your organization must include a plan for monitoring and testing that includes either (i) continuous monitoring or (ii) periodic penetration testing and vulnerability assessments. Penetration testing is defined under the regulations as "a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside [your] information systems," and must be conducted at least annually. Penetration testing (and the plan to conduct such testing) should focus on the relevant risks that are identified in your organization's Risk Assessment, as described in further detail below. Vulnerability assessments, which are to be conducted on a biannual basis, should likewise be based on the results of your organization's Risk Assessment, and include any systemic scans or review of information systems reasonably designed to identify publicly known cybersecurity vulnerabilities that may exist in your information systems.

It is important to note that NYDFS does not require that the penetration testing and vulnerability assessments be completed by March 1, 2018. Rather, your organization needs to have a plan in place by that date that provides for penetration testing and vulnerability assessments to be completed in a timely manner going forward.

Risk Assessment (Section 500.09)

Under the Cybersecurity Regulation, risk assessments should be carried out in accordance with your organization's written policies and procedures and are required to include (i) criteria for the evaluation and categorization of cybersecurity risks or threats to your organization; (ii) criteria for assessing the confidentiality, integrity, security, and availability of your organization's information systems and nonpublic information; and (iii) requirements describing how identified risks will be mitigated or accepted, and how your organization's cybersecurity program will address the risks. Risk assessments should be considered "living" documents, and should be updated to address any changes to your information systems, nonpublic information, or business operations of your organization or any subsidiary or other affiliate that may present risks to your organization's information systems or the nonpublic information stored on such systems. Risk assessments should also be updated in response to technological developments and evolving threats.

We note that unlike the clarification provided in NYDFS's FAQs that covered entities must have a plan in place to conduct penetration testing by March 1 (but not necessarily have completed the actual testing by this date), NYDFS has provided no guidance as to whether conducting the Risk Assessment must be completed by March 1, 2018 (as opposed to having a plan to complete the Risk Assessment in a timely manner). At a minimum, organizations should have a Risk Assessment plan in place by the March 1, 2018 deadline.

Multi-Factor Authentication (Section 500.12)

Under the framework put forward by the Cybersecurity Regulation, your Risk Assessment will inform your determination of effective controls, which may include multi-factor authentication or risk-based authentication. Pursuant to the Cybersecurity Regulation, multi-factor authentication should be utilized by any individual accessing your internal networks from an external network unless your CISO provides written approval for equivalent or more secure access controls. Your risk assessment should also determine the appropriate controls for third party service providers, which may result in such organizations using multi-factor authentication if access is required to your organization's internal networks.

Cybersecurity Awareness Training (Section 500.14(b))

The Cybersecurity Regulation requires that your personnel receive regular cybersecurity awareness training. This training should be updated over time to reflect your organization's risks as identified in your Risk Assessment.

We note the same caveat mentioned earlier with regards to the Risk Assessment, that NYDFS has provided no guidance as to whether all personnel must have received cybersecurity awareness training by March 1, 2018 (or simply that a plan for cybersecurity training must be in place). In any case, organizations will want to confirm personnel receive regular training, particularly as updates are made to your Risk Assessments to reflect the evolving threat landscape.

The one-year transitional period that ends on March 1, 2018, marks another significant implementation milestone for the NYDFS Cybersecurity Regulation. The next key date will be September 3, 2018, when covered entities are required to be in compliance with provisions related to the following: Audit Trail; Application Security; Limitations on Data Retention; Monitoring; and Encryption. The final transitional period ends on March 1, 2019, when covered entities must be in compliance with the requirements regarding written security policies applicable to third party service providers.

Please let us know if you have any questions, or if we can be of assistance in these matters.

Contacts

Harriet Pearson
Partner, Washington, D.C., New York
T +1 202 637 5477
harriet.pearson@hoganlovells.com

Gregory Lisa
Partner, Washington, D.C., New York
T +1 202 637 3647
gregory.lisa@hoganlovells.com

Aleksander Dukic
Partner, Washington, D.C.
T +1 202 637 5466
aleksander.dukic@hoganlovells.com

Deen Kaplan
Partner, Washington, D.C.
T +1 202 367 5799
deen.kaplan@hoganlovells.com

Beth Peters
Partner, Washington, D.C.
T +1 202 637 5837
beth.peters@hoganlovells.com

Tim Tobin
Partner, Washington, D.C.
T +1 202 637 6833
tim.tobin@hoganlovells.com

Stephenie Gosnell Handler
Senior Associate, Washington, D.C.
T +1 202 637 5540
stephenie.handler@hoganlovells.com

Paul Otto
Senior Associate, Washington, D.C.
T +1 202 637 5887
paul.otto@hoganlovells.com

Marc Gottridge
Partner, New York
T +1 212 909 0643
marc.gottridge@hoganlovells.com

A special thanks to Asmaa Awad-Farid for her contribution to this alert.

www.hoganlovells.com

"Hogan Lovells" or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.
The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.
For more information about Hogan Lovells, the partners and their qualifications, see www. hoganlovells.com.
Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.
© Hogan Lovells 2018. All rights reserved.