Drinker Biddle

Client Alert

December 29, 2016

NYDFS Proposes Revised Cybersecurity Requirements for Financial Services Companies

By Thomas M. Dawson and Yuliya Feldman

The New York Department of Financial Services has released an extensively revised cybersecurity regulation applicable to the wide variety of financial services companies regulated by the NYDFS. Released on December 28, 2016, the revised regulation makes multiple changes to almost every provision in the original proposal. We summarized the original proposed regulation in a Client Alert issued on September 14, 2016 and subsequently helped re/insurance clients submit comments to the NYDFS. Industry cybersecurity experts will undoubtedly take some time to consider all of the implications of the many changes made by NYDFS drafters. On the whole however we suspect that many financial companies that knew they were squarely targeted as "covered entities" will be pleased to see that the NYDFS has incorporated risk-based regulatory concepts in many of the requirements retained in the revised proposal.

At the same time there will be others—particularly non-U.S. reinsurers that are "certified" or "accredited" by the NYDFS and that are subject to home country cybersecurity regulatory requirements—that will not be pleased to see absolutely no change in the definition of "covered entity." The NYDFS asserts that its definition of "covered entity" was clear; that it may be. The real point is that it is overbroad and extraterritorial in its application—evidencing a return to regulatory practices of the past with respect to reinsurance (practices that were reversed by Title V of the Dodd-Frank legislation).

Our overview of the changes made and the key takeaways regarding the impact the revised regulation could have on participants in the insurance industry follows.

Background

In September 2016, the NYDFS proposed "First-In-The-Nation" cybersecurity requirements for financial services companies. This long-awaited proposal was the culmination of an effort by the NYDFS to address cybersecurity risks posed to its regulated entities. After receiving over 150 comments on the proposed regulation, the NYDFS made numerous changes to address concerns raised in those comments.

The Framework Remains

The general categories of cybersecurity requirements in the revised proposed regulation have remained the same and include the following:

- Maintaining a cybersecurity program, including the adoption of a written cybersecurity policy;
- Implementing and maintaining written policies and procedures regarding application security, data retention, and information systems and nonpublic information accessible to or held by third party service providers;
- Periodically (not annually) assessing information systems;
- The designation of a qualified individual to function as Chief Information Security Officer (CISO) and the CISO's responsibilities;
- Employment and training of cybersecurity personnel and training for all personnel;
- Technical requirements, including multi-factor authentication and encryption of nonpublic information;
- Oversight requirements including penetration testing, vulnerability assessments, risk assessments, and audit trail systems;
- Establishment of a written incident response plan and notification to the superintendent in the event of a cybersecurity event; and

- Annual certification (the "Certification of Compliance") by senior executives (or possibly by entire Boards of Directors) to the NYDFS Superintendent of compliance with the cybersecurity regulation.

The Revised Regulation

Notable changes include the following:

- **Risk-Based Approach**. The required "periodic" (it was annual) risk assessment of a covered entity's information systems is no longer just an oversight requirement, but is now envisioned as the foundation of each regulated entity's dynamic plan to address its own business operations, including the use, maintenance and security of nonpublic information. Many requirements, including the cybersecurity program, the cybersecurity policy, penetration testing and vulnerability assessments, audit trails, third party service provider security polices, multi-factor authentication, and encryption, are now to be based on the Covered Entity's own periodic risk assessments. Additionally, the NYDFS has softened language around certain requirements. In many places, where the original requirements were to apply "at a minimum," they are now required "to the extent applicable."

- **Definition of Nonpublic Information**. The definition of "Nonpublic Information" was substantively changed. Generally, the definition was narrowed from the original.

- **Third Party Service Provider Security Policy**. The revised proposed regulation provides more risk-based flexibility for a Covered Entity's interaction with third party service providers regarding cybersecurity "to the extent applicable."

- **Exemptions.** The exemptions were expanded but the "small covered entity" exemption remains unchanged. Notably, there is a new exemption for a "Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information…" A Covered Entity that fits this exemption will be exempt from many, but not all, of the cybersecurity requirements.

- **Notice of Exemption**.The revised proposed regulation requires a Covered Entity that qualifies for an exemption to file a Notice of Exemption with the NYDFS.

- **Additional Flexibility to Use Cybersecurity Resources of Others**.The revised proposed regulation allows a Covered Entity to use an affiliate's cybersecurity program to satisfy the cybersecurity requirements. Additionally, an exemption was created for "[a]n employee, agent, representative or designee of a Covered Entity, who is itself a Covered Entity" to the extent that such a person is covered by the cybersecurity program of the Covered Entity. Indeed, an entity's CISO need not even be an employee but instead may be employed by an affiliate or by a third party service provider.

- **Effective Date and Transitional Period**.The Effective Date was changed to March 1, 2017, with the first Certification of Compliance being due on February 15, 2018. Additionally, the revised proposed regulation introduces extended transitional periods for certain cybersecurity requirements. A summary of the extended transitional periods follows. The general transitional period, unless otherwise extended as shown in the chart below, is 180 days from March 1, 2017.

Extended Transitional Period Summary

1 Year	18 Months	2 Years
CISO's First Report to the Board of Directors Penetration Testing and Vulnerability Assessments Risk Assessment Multi-Factor Authentication Cybersecurity Training for All Personnel	Audit Trail Application Security Limits on Data Retention Policies, Procedures and Controls for Monitoring Activity of Authorized Users Encryption	Third Party Service Provider Security Policy

Some other changes include the following:

- The addition of a definition of "Third Party Service Provider(s)";

- Changes to various applicable time periods (e.g., the CISO previously had to report at least twice each year to the Board of Directors and now must report annually);

- Narrowing of the audit trails to be maintained;

- Simplification of the multi-factor authentication requirements;

- Providing more flexibility when encryption is infeasible; and

- Addition of a confidentiality provision with respect to filings made with the NYDFS.

Takeaways

As already noted, the revised proposed regulation includes multiple changes to almost every provision in the original version. We are happy to provide detailed advice on any of these upon request.

It is worth stressing that one provision that has not changed is the definition of "covered entity." Leaving it unchanged to apply to anyone "operating pursuant to a license, registration, charter, certificate, permit, accreditation or similar authorization" will capture a very wide range of lightly regulated entities (e.g. service contract providers) or entities regulated by home country regulators (e.g. some but not all non-U.S. reinsurers).

Generally, many of the changes made demonstrate an attempt by the NYDFS to tailor and provide some risk-based flexibility to regulated entities in complying with the cybersecurity requirements. How far these adjustments will go in making these requirements workable for Covered Entities is yet to be determined.

Indeed, how well will the NYDFS standards harmonize with the yet-to-be-released NAIC Data Security Model Law/Regulation? How will New York's framework fit with Version 1.1 of the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity due to be published early in 2017? While NIST's Version 1.1 will continue to be voluntary, the possibility exists that the NAIC or other states (or other countries) could develop binding cybersecurity standards and requirements for insurers and other regulated entities that deviate from --or conflict with-- those about to go into effect in New York. That balkanization would be in no one's interests.

* * * * *

The revised proposed regulation is subject to a 30-day notice and public comment period before its final issuance. However, the NYDFS has asserted that it carefully considered all of the comments submitted during the previous comment period and incorporated those suggestions that it deemed appropriate. Therefore, during this second comment period, the NYDFS will focus only on "new" comments.

Insurance Regulatory and Transactional Team

Primary Contacts

Thomas M. Dawson
Partner
New York | London
(212) 248-3160
Thomas.Dawson@dbr.com

Yuliya Feldman
Associate
New York
(212) 248-3172
Yuliya.Feldman@dbr.com