New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 261—NO. 64
THURSDAY, APRIL 4, 2019

Outside Counsel

New York's Cyber Regulation Two Years Later: We've Only Just Begun

By **Craig A. Newman**

And **Kade N. Olsen**

Financial institutions regulated by New York's Department of Financial Services (DFS) can breathe a sigh of relief, at least temporarily. Two years after DFS's "Cybersecurity Requirements for Financial Institutions" took effect, and more than three years after the cybersecurity regulation was announced, the final provision of the law became effective on March 1 of this year.

But the celebrations must be short. DFS got it right when describing its then-new regulation as the "first in the nation." Like the federal Sarbanes-Oxley Act of 2002, financial institutions will have to certify annually that their internal controls and cybersecurity practices remain up to snuff. And now that the transitional periods for implementing the cyber regulation have passed, covered institutions will need to certify that they have complied with each provision.

CRAIG A. NEWMAN *is a partner and* KADE N. OLSEN *is an associate at Patterson Belknap Webb & Tyler.*

Some of those requirements are one-off. For example, §500.04 required each covered entity to "designate" a Chief Information Security Officer or CISO. And §500.16 required companies to establish an Incident Response Plan. Absent changes at the company or a need to update compliance, covered entities will not have much to do on a day-to-day basis when it comes to these two requirements.

But those one-time provisions are the exception. For the rest of the regulation, covered entities will need to check (and then re-check) their cybersecurity controls, policies and practices in order to remain in compliance.

The regulation's ongoing obligations can be broken into three categories—provisions that: (1) have set deadlines; (2) mandate "periodic" action; and (3) require near-constant attention.

Set Deadlines

There are a handful of provisions that require companies to take action on a predictable and regular basis:

• **Vulnerability Assessments:** Section 500.05(b) requires, for those companies that do not perform continuous monitoring on their network, to conduct "*bi-annual* vulnerability assessments, including systematic scans or reviews of Information Systems." Under the regulation, "Information Systems" means a company's information technology environment including its network.

Now that the transitional periods for implementing the cyber regulation have passed, covered institutions will need to certify that they have complied with each provision.

• **Penetration Testing:** §500.05(a) requires, again for those companies that do not use continuous monitoring, the performance of *annual* penetration testing.

• **CISO Report:** §500.04(b) requires the CISO, "at least *annually*," to provide a written report to the organization's board of directors or equivalent governing body, covering a variety of topics that are spelled out in the regulation.

• **Encryption Alternatives:** §500.15(b) requires, for those companies employing alternative compensating controls instead of encryption, the CISO to consider *annually* "the feasibility of encryption and effectiveness of the compensating controls."

• **Compliance Certification:** As most covered entities should know by now, *annually* each company must submit a certificate of compliance to DFS attesting to the organization's compliance with the regulation for the past fiscal year.

• **Exemption Certification:** Although the text of the regulation does not require companies qualifying for a limited or complete exemption to "re-file" their exemption, according to DFS's website, companies must re-file their notice of exemption *every two years*.

Periodic Obligations

Several of the regulation's provisions require "periodic" review and action. To date, DFS has yet to define what "periodic" means, and it's unlikely that the agency will do so. As the previous examples demonstrate, when DFS wants to set hard-and-fast deadlines, it knows exactly what to do. Accordingly, companies will need to use their own judgment to decide when to take action based on their own circumstances, risk profile and on a provision-by-provision basis.

• **Risk Assessment:** For companies that conducted their first risk assessment in 2018 to comply with §500.09, more work is likely on the horizon. The regulation requires companies to conduct "a periodic" risk assessment. At a minimum, institutions should update their risk assessment in response to changes to their information security systems or data security environment, which could include various scenarios such as migrating to the cloud, launching a public-facing website, or merging with a new company.

But the risk assessment itself is only half of the equation. Many of the regulation's requirements are keyed off of the risk assessment: §500.03's policy obligations, §500.06's audit trail requirements, and §500.15's encryption mandates—just to name a few—are all subject to an organization's risk assessment. When companies conduct a periodic risk assessment, they will need to carefully review and evaluate their cybersecurity program in light of whatever findings are made.

• **Access Privileges:** §500.07 requires that companies "periodically review … access privileges." Access privileges, as the name suggests, determines who can access parts of a company's network, and should be monitored on a regular basis. And the "periodic" nature of the review might change depending on the scenario. For example, companies might remove user access privileges *immediately* for those who part ways with the company. On the other hand, a company could review (and alter as needed) the access privileges of current users on a monthly or quarterly basis.

• **Data Retention:** Finally, companies must "dispos[e] on a periodic basis of any Nonpublic Information" that is "no longer necessary" for "business operations or for other legitimate business purposes." Whatever periodic timeframe an organization choses, DFS requires that it be identified in its written "policies and procedures."

Constant Compliance

Last, but certainly not least, are the regulatory requirements that affect an organization's day-to-day operations. These can be broken down into a handful of categories:

• **Maintenance:** Several provisions in the regulation require companies to "maintain" their cybersecurity environment and cybersecurity policies. First and foremost,§500.02 requires covered

entities to "maintain" a "cybersecurity program designed to protect the confidentiality, integrity and availability" of their information systems. As DFS has explained in a recent memo, it expects companies to treat cyber issues as a "governance issue," and as a result, companies would be well advised to regularly review and evaluate the effectiveness of their cybersecurity program.

The regulation uses the same verb—"maintain"—in its description of an organization's audit trail obligations. In §500.06, DFS mandates that entities must "securely maintain systems" that are "designed to reconstruct material financial transactions." In conjunction with the retention obligation for that provision ("not fewer than five years"), the regulation appears to expect companies to continually ensure they have sufficient information to reconstruct business-critical financial transactions on a trailing five-year basis.

• **Breach Notices:** As companies that have suffered a data security incident—or "Cybersecurity Event"—know, §500.17 imposes an accelerated reporting deadline. No "later than 72 hours from a determination" that a qualifying event has occurred, companies must provide DFS with notice. Beating the 72-hour shot-clock requires established chains of communications between companies' IT employees and their compliance teams.

• **Third-Party Service Providers.** As other commentators have discussed at length, the most time-consuming and demanding provisions of the cybersecurity regulation are those governing companies' interactions with third-party vendors.

Part (a) of §500.11 could be handled in one swoop. Using their risk assessments, companies must "implement written policies and procedures" designed to ensure the security of information systems and nonpublic information accessible to third parties. Those policies must cover the identification of risk, minimum cybersecurity practices, due diligence processes and periodic assessments.

> The conclusion of the "transitional period" for New York's cybersecurity regulation marks the beginning, rather than the end, of an organization's compliance efforts.

But, from there, the §500.11's obligations go outward and onward. Subsection (b) calls for "guidelines for due diligence and/or contractual protections relating to Third Party Service Providers." This language suggests that DFS expects companies to review and evaluate their vendors and contracting parties with access to their network or sensitive information. Indeed, in response to an FAQ posted on the DFS website, the agency emphasized that covered organizations should perform "a risk assessment regarding the appropriate controls for Third Party Service Providers based on the *individual facts and circumstances* presented and does not create a one-size-fits-all solution." Accordingly, for each contract in which a third party has access to a covered entity's information systems or nonpublic information, DFS expects a certain level of due diligence and "contractual protections" governing cybersecurity, subject to the organization's risk assessment process.

Conclusion

The conclusion of the "transitional period" for New York's cybersecurity regulation marks the beginning, rather than the end, of an organization's compliance efforts. Although financial institutions might be fully compliant today, that could easily change absent ongoing diligence and monitoring.