Compliance Deadline Looms On State Cybersecurity Regulation

The new law requires strong governance. NACD principles can help.

By Judy Selby and Steven R. Chabinsky

THINKSTOCK/GETTY IMAGES

New York state's powerful financial regulator, the Department of Financial Services (DFS), recently grabbed headlines by issuing "Cybersecurity Requirements for Financial Services Companies." The regulation, which went into effect on March 1, sets out a long list of cybersecurity "minimum standards" for companies that directly fall under DFS's purview. Significantly, the word "minimum" in this context does not mean nominal. Similarly, the word "standards" does not mean guidance. Rather, regulated companies are finding the requirements to be numerous, exacting, and resource-intensive. Corporate officers and directors, beware.

The first thing an organization must do is determine whether the regulation applies to it. The answer may not be immediately obvious, because the cybersecurity regulation does not simply impact those companies (and individuals) directly subject to New York state's financial, banking, or securities law. The regulation also impacts those companies that provide network infrastructure and information security services to affiliates (such as subsidiaries or agents) operating under New York's supervision. It is the impact of this latter category—which requires a review of an organization's cybersecurity functional structure—that has proven most eye-opening, and at times jaw-dropping, in its ramifications.

Fortunately, directors can fulfill their duties under New York's regulation by applying the five core principles of the National Association of Corporate Directors' (NACD) *Handbook on Cyber-Risk Oversight*.

PRINCIPLE 1 **Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue.**

The DFS regulations implement a risk management approach. The new regulation demands strong governance from individuals both within and outside of the information technology and security teams, going all the way to the board. Starting in February 2018, senior management or the board itself must file an annual certification confirming compliance with the regulation. Similarly, senior management or the board must approve the company's formal, written cybersecurity policies—which must address 14 distinct areas that range from information security to incident response.

In short, there is no room for doubt among leadership. According to DFS, "Senior management must take this issue seriously and be responsible for the organization's cybersecurity program." Meeting this obligation will require board expertise and attention.

PRINCIPLE 2 **Directors should understand the legal implications of cyber risks specific to their company's circumstances.**

Cyberevents are typically evaluated by the impact they have on the confidentiality, integrity, and availability of compromised data or systems. The magnitude of harm from an incident is entity-specific, and can change based on the quantity and quality of the data an organization acquires, retains, and transfers, and the types of services it deploys. The typical legal and financial implications include litigation and regulatory fines, reputational damage, business disruption, and the costs of response, recovery, and remediation.

Getting cybersecurity wrong for a DFS-supervised entity now becomes an added potential liability. Although DFS does not spell out specific fines or penalties associated with violations, the regulation provides that it will be enforced pursuant to DFS authority "under any applicable laws," and we understand that DFS

examiners are being trained on the new regulation. Of course, there's also the potential for director liability. Following a breach, directors are sure to be questioned about what they knew about the adequacy of the company's internal cybersecurity controls, whether any material gaps existed, and what the directors did or failed to do about them. New York-supervised companies must report certain types of events to DFS within 72 hours, and boards should have confidence that they will receive notice of those reports as well.

PRINCIPLE 3 **Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be a regular part of the board meeting agenda.**

Documented, engaged, continuous, and informed oversight by the board is crucial to protect an entity against cybersecurity threats and liabilities, as well as to ensure compliance with the New York regulation. To be informed, boards require resident expertise or outside advisors who can help them ask the right questions, and understand the answers and the need for follow-up. Under the new regulation, the board should demand a written report from the now-required chief information security officer (CISO), assessing risk based on the following considerations:

- the confidentiality of the institution's sensitive personal and business information;
- the integrity and permeability of systems;
- the entity's policies and procedures;
- its material cybersecurity risks;
- overall cybersecurity effectiveness; and,
- material cybersecurity events during the reporting period.

Boards should know in advance whether DFS compliance will be discussed separate from, or included within, the typical cadence for addressing data privacy and cybersecurity matters, or only upon receipt of the CISO report. Boards also should identify which directors or committees are expected to assess the CISO's report and address any changes it reflects to the company's risk exposure.

PRINCIPLE 4 **Directors should expect management to establish an enterprise-wide cyber-risk management framework.**

Under the regulation, each covered entity must conduct a periodic risk assessment that is expected to inform the company's entire cybersecurity program. The risk assessment must be documented and updated as needed to account for material changes in the company's profile, recent technological developments, and evolving threats. Preparing the risk assessment requires a formal process that, at a minimum, includes:

- criteria for evaluating and categorizing identified cybersecurity risks or threats;
- criteria for assessing the confidentiality, integrity, security, and availability of the company's information systems and nonpublic information;
- criteria for measuring the adequacy of existing controls in the context of identified risks; and,
- requirements describing how identified risks will be mitigated or accepted based on the results of the risk assessment.

Perhaps the most groundbreaking part of the regulation is the requirement for annual, written certifications of compliance, signed either by the board chair or a senior officer. Whoever signs that document is expected to certify to the best of their knowledge either that the entire board, or one or more specific named senior officers, "reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors, and other individuals or entities as necessary" to comply with the regulation.

PRINCIPLE 5 **Board-management discussion of cyber risks should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance.**

Also consistent with NACD principles, DFS requires regulated companies to document the identification of any "areas, systems or processes that require material improvement, updating or redesign," together with the remedial efforts planned or underway to address them. This is consistent with the principle that cyber risks will be mitigated or accepted based on the company's risk assessment. Although some identified risks can be transferred through cybersecurity insurance, much of it cannot, and it's important for a company to keep up on changes within the insurance market as well.

A board also should be familiar with the company's method of documenting its DFS compliance and responding to any DFS requests, with an understanding that all of the documentation and information relevant to the company's cybersecurity program must be made available to New York upon its request.

In short, there's a lot to be documented, and potentially a lot to be disclosed and defended under New York's first-of-its-kind cybersecurity regulation. Corporate officers and directors are only now beginning to understand this new reality, and there is not much time to waste. The regulation's transitional timeline includes significant milestones that must be reached by Aug. 28, 2017. The time for director oversight is now. Get a head start by reading NACD's *Directors' Handbook on Cyber-Risk Oversight*.

Judy Selby is managing director of insurance and technology advisory services at BDO USA. Steven R. Chabinsky is a partner at White & Case and chair of the firm's global data, privacy, and cybersecurity practice.