Debevoise & Plimpton

Insurance Industry Corporate Governance Newsletter

To Our Clients and Friends

The last edition focused on developing disclosure rules regarding climate change risk and investments and how regulators and shareholders are responding to the growing body of disclosure requirements. These new disclosure rules have wide-ranging implications for the industry and have proven to be an increasing source of potential liability.

This month, we examine the draft amendments to the Part 500 Cybersecurity Rules proposed by the New York Department of Financial Services (the "NYDFS") on July 29, 2022. The amendments include significant changes relating to governance, technology, risk assessments, notifications, and penalties. Here we provide a high-level overview of the proposed changes, with a focus on the aspects of the amendments most critical to general counsel, other C-suite executives and board members so that they both can understand the impact of the new amendments and decide whether their respective companies should comment.

There will be a very short pre-proposal comment period (ending August 18, 2022), followed by the publishing of the official proposed amendments in the coming weeks, which will start a 60-day comment period.

Overview of the Existing Regulation

In 2017, the New York Department of Financial Services published Part 500, the Cybersecurity Rule. The rule was one of the very first regulations focusing on cybersecurity and laid out distinct governance, technology and regulatory notification requirements for covered entities and their vendors. It was also one of the first cybersecurity rules requiring an annual certification of compliance.

The 2017 regulation was a risk-based regulation, allowing companies to largely tailor their program to the risks they faced. The regulation did not start out as risk-based. NYDFS issued an initial draft and made great effort to interact with the industry to shape the regulation to something very workable. The final version was hailed as a meaningful but reasonable law that served as a model for cybersecurity regulation for many other agencies, and the most current version of the regulation has a number of governance provisions. For example, each covered entity must have a cybersecurity program, the board of directors must receive a yearly report about the cyber program, a senior executive must be responsible for the cyber program and a senior executive must sign the yearly certification of compliance with the regulation.

Importantly, the proposed amendments contain significant new governance obligations that the general counsel, C-suite and board should consider and that we outline below.

Board and CEO Obligations

- **Board Reporting**: Under the current regulations, the Chief Information Security Officer must provide a yearly report to the board. The CISO must consider certain elements of the enterprise's cybersecurity in formulating the report, but there are no requirements as to the actual contents of the report. The proposed amendments change that by specifying the materials that the board must see. The CISO also now has an obligation to brief the board on plans for remediating inadequacies, as

well as a requirement for timely reporting to the board on material cybersecurity issues or major cybersecurity events.

- **Board Expertise**: Consistent with the SEC's focus on the cybersecurity expertise of board members, under the draft amendments, the board of covered entities will be required to have sufficient expertise and knowledge (or be advised by persons with sufficient knowledge and expertise) to exercise effective oversight of cyber risk.

- **Policy Approvals**: Under current regulations, a senior officer of the covered entity must approve the company's cybersecurity policies. The proposed amendments change that, requiring the board to approve those policies.

- **CISO Independence**: The draft amendments require that the CISO have adequate independence and authority to ensure that cyber risks are appropriately managed. While that independence is not defined, in the past there has been discussion in cybersecurity governance circles about the CISO reporting outside of technology, e.g., to the COO or even the general counsel, either directly or by a dotted line in the org. chart.

- **CEO Certification**: To date, the annual certification of compliance needed to be signed by a senior officer. Many companies tapped the CISO or COO for this role. Under the draft amendments, both the CEO and the CISO would need to certify compliance. In addition, under the current rules, the certification is only signed if the company is in complete compliance. The new rules, however, would allow for an acknowledgement of less-than-full compliance, with an identification of the specific deficiencies. Companies that cannot certify full compliance will therefore need to be prepared to provide the NYDFS with their documentation of remedial efforts planned and underway, along with a timeline for implementation of those efforts.

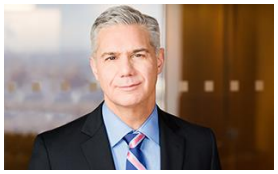
- **Tabletop Exercises and Incident Response Plans**: Under the proposed amendment, covered entities must periodically test their incident response plans with all staff who are critical to the response. The proposed amendment specifically calls for the CEO to participate in such testing (typically through tabletop exercises).

Risk Assessments

General counsel may also want to focus on the significant new requirements for risk assessment, which provide that they must be tailored to the company in light of its size, staffing, governance, services, products, vendors, locations and other factors. They also need to include a threat and vulnerability analysis. Many companies now work with outside counsel and external consultants to conduct risk assessments. In doing so, the companies are able to gain a comprehensive benchmarking of the program, a summary of which can be very helpful to the board of directors. Additionally, by including counsel, the technical results of the consultant review can be mapped to regulations such as Part 500 and others.

Conclusion

The proposed amendments to Part 500 include many changes that may require the general counsel's attention. In addition to the above, there are new requirements for large companies, which can include smaller covered entities with large affiliates. Given the NYDFS's history of working with industry to improve Part 500, there is every reason to think that submitting comments to the Department during the comment periods can be fruitful.



Eric R. Dinallo
Partner
+1 212 909 6565
edinallo@debevoise.com

Erez Liebermann
Partner
+1 212 909 6224
eliebermann@debevoise.com

Nicolas F. Potter
Partner
+1 212 909 6459
nfpotter@debevoise.com

Charu Chandrasekhar
Counsel
+1 212 909 6774
cchandrasekhar@debevoise.com