Debevoise & Plimpton | Insurance Industry Corporate Governance Newsletter

To Our Clients and Friends,

The last edition of our Insurance Industry Corporate Governance Newsletter focused on the changes of the Net Zero Insurance Alliance ("NZIA"), explaining the original idea behind the formation of NZIA, why it was appealing as a matter of insurance companies' corporate governance, and why now so many companies that initially signed up for the NZIA have announced their departure.

This month's edition focuses on recent developments in cybersecurity regulations for public insurance companies. As cyber threats continue to pose major risks to the insurance industry, regulators are imposing more requirements intended to strengthen cybersecurity risk management and governance, as well as related disclosures. Two key regulatory regimes for insurance industry participants are the cybersecurity rules adopted by the New York Department of Financial Services ("NYDFS") and the U.S. Securities and Exchange Commission ("SEC"). In June and July, respectively, the NYDFS announced revised proposed updates to its cybersecurity regulations, and the SEC adopted long-anticipated final cybersecurity rules for issuers.

As we discuss below, the two regimes pose distinct challenges for insurance industry participants, and may also be in tension—adding complexity for companies that must comply with both the NYDFS and SEC cybersecurity rules, especially when investigating and potentially disclosing a cybersecurity incident.

NYDFS and SEC Cybersecurity Rules: What Are They and Why Do They Matter?

While the subject matter and goals of these regulations are similar, there are important differences in their implementation, which is a product of different regulatory toolkits at the NYDFS and SEC. The NYDFS, as a prudential regulator, enacted prescriptive rules, establishing what has become the *de facto* cybersecurity standard for insurance companies nationwide. On the other hand, the SEC's rules are intended to, in Chair Gary Gensler's words, "enhance and standardize disclosures to investors with regard to public companies' cybersecurity practices as well as material cybersecurity incidents."

In effect, the NYDFS set forth the cybersecurity standards insurance industry participants must operationalize, and the SEC will now require those internal practices to be more fully disclosed.

The NYDFS Cybersecurity Rule and Proposed Amendment

When the NYDFS cybersecurity rules were first enacted in 2017, they were widely regarded as the most comprehensive cybersecurity regulations in the United States. The NYDFS rules detail cybersecurity requirements in several specific areas, including personnel, training, policies, access privileges, penetration testing, encryption, multifactor authentication, application security, data minimization and vendor management.

On June 28, 2023, the NYDFS announced its Revised Proposed Second Amendment to these cybersecurity rules, which reflects revisions made by the NYDFS as a result of comments it received on its Initial Proposed Second Amendment released in November 2022.

The amendment proposes to create a new category of "Class A companies" to whom substantial additional cybersecurity requirements will apply. Although the revised proposed amendment would narrow the definition of Class A company, most major insurance companies with operations in New York will continue to be covered by enhanced compliance obligations, such as annual independent audits of their cybersecurity program and implementation of sophisticated access management, endpoint detection and event logging systems.

The amendment also enhances or adds a number of cybersecurity requirements for all regulated entities, such as expanded NYDFS incident notification obligations, universal multifactor authentication, and annual penetration testing. From a governance perspective, the proposed amendment mandates board oversight of cybersecurity risk, including annual review and approval of cybersecurity policies and reporting by the CISO to the board, and requires the board to "have sufficient understanding of cybersecurity-related matters to exercise such oversight."

SEC Adopts Cybersecurity Rules for Issuers

On July 26, 2023, the SEC adopted long-anticipated rules on cybersecurity risk management, strategy, governance and incident disclosure for issuers. The SEC issuer rules create new public reporting obligations relating to cybersecurity incidents and risk management for all public companies. The new rules are part of the SEC's larger efforts focused on cybersecurity, with a growing ecosystem of cybersecurity rules aimed at different types of SEC registrants.

The SEC rules introduce three new categories of required disclosure: (1) material cybersecurity incidents; (2) cybersecurity risk management processes; and (3) cybersecurity oversight and governance.

Material cybersecurity incidents: The SEC issuer rules create an obligation to disclose cybersecurity incidents within four business days of determining an incident is material. Amended or updated disclosures may also be required when information becomes available after initial disclosure, or if an issuer discovers a material error in previously disclosed information.

Cybersecurity risk management processes: The SEC issuer rules require disclosure of more details about cyber risk management processes than is common among public companies at present.

Cybersecurity oversight and governance: The SEC issuer rules require disclosure about the roles that management and the board play in managing and overseeing cybersecurity risk, and granular details regarding management's cybersecurity expertise.

How Will the NYDFS and SEC Rules Work Together?

These distinct approaches to regulation mean there are not significant overlapping requirements between the two regimes. However, there are important interactions, and potential tensions, for insurance industry participants required to comply with both frameworks.

For example, the NYDFS requires a broad set of cybersecurity incidents to be reported to the regulator within 72 hours. The SEC rules, on the other hand, require public disclosure of cybersecurity incidents within four business days of determining the incident is material. While the reporting of an incident to a regulator is not dispositive of materiality, the risk of regulatory action is one factor the SEC believes should be weighed in making the materiality determination. Moreover, any information about a cybersecurity incident reported to the NYDFS should be consistent with public disclosure (if any) about the incident, putting greater pressure on swift discovery of facts and necessitating close coordination across information technology, legal and compliance functions.

Furthermore, NYDFS-required processes to manage cyber risk, board and management oversight of cyber risk, and policies and procedures relating to cybersecurity risk will become subject to public disclosure. As a result, the processes implemented to comply with the NYDFS may be subject to greater scrutiny from other stakeholders, in addition to NYDFS supervision.

The SEC rules will require so-called "block tagging" of the newly required cyber disclosures using machine-readable XBRL. The use of XBRL greatly increases the ease of aggregating and comparing disclosure across large numbers of issuers, a technique widely used by the SEC and other securities market participants. This ease of access could lead to additional comparison and scrutiny across public insurance companies, and further merging of best practices and expectations for cybersecurity risk management, in addition to the standardization of disclosure.

When Is Compliance Required?

The amended NYDFS cyber rule is expected to become effective this Fall.

The SEC cyber rule will begin to phase in later this year, beginning with Form 8-K disclosure of material cybersecurity incidents in December 2023 and cybersecurity risk management and governance disclosure required for most calendar year-end issuers in their next Form 10-K (filed in early 2024). Inline XBRL tagging must begin one year after initial compliance with the related disclosure requirement.

What Steps Should Issuers Take Now?

Insurance industry participants should begin assessing their cybersecurity capabilities now, to identify any gaps in their ability to comply with proposed NYDFS technical requirements.

Because cyber incidents may unfold rapidly and unpredictably, strict adherence to internal practices and disclosure controls and procedures supporting a well-informed and deliberative materiality analysis will help issuers demonstrate good faith compliance with their disclosure obligations. Issuers should develop and test robust disclosure controls and procedures prior to a "live" cybersecurity incident to ensure that cybersecurity Form 8-K disclosure decisions—which will be uniquely challenging, as they will typically require input from multiple technical, business and legal stakeholders, and will often relate to rapidly developing cybersecurity investigations—can be made swiftly and accurately.

Processes for managing and overseeing cybersecurity risk should be reviewed and benchmarked against industry standards. Issuers should consider how these processes are integrated with their overall risk management program, and relate to their cyber risk profile, to consider how required disclosures will appear in the face of greater public scrutiny.

Enhanced disclosure about senior management and the board will up the ante on expectations for cybersecurity oversight and put more pressure on issuers to attract, develop and retain cybersecurity talent. Issuers should review cybersecurity talent and capabilities, and identify any gaps where outsourcing or additional talent development is needed.

Ensuring that both senior management and the board are informed, and that their involvement is well-documented, will be more important than ever. Issuers should consider the substance and frequency of cybersecurity reporting to management and the board.

Conclusion

The continued focus on cybersecurity risks by both the NYDFS and SEC highlights the importance of good corporate governance and robust risk management programs addressing cybersecurity. The SEC rules also reinforce the importance of developing dynamic disclosure controls and procedures that are geared to manage cybersecurity incident disclosure in fluid situations, across a rapidly evolving threat landscape. Implementation of processes to comply with these interrelated and complex rules should be a priority for public insurance companies, their management and boards of directors.

To subscribe to our Data Blog, please click here.

Charu A. Chandrasekhar
Partner
+1 212 909 6774
cchandra@debevoise.com

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

Avi Gesser
Partner
+1 212 909 6577
agesser@debevoise.com

Benjamin R. Pedersen
Partner
+1 212 909 6121
brpedersen@debevoise.com

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