HINSHAW

News

Via FinOps Report: Cathy Mulrow-Peattie Discusses NYDFS Cybersecurity Regulation Implications for the Financial Services C-Suite

February 15, 2024

Cathy Mulrow-Peattie was recently featured in *FinOps Report*, discussing New York State's amended cybersecurity regulation and its implications for C-level executives, particularly financial services company management. The regulation requires CEOs, CISOs, and boards of directors to take a more active role in overseeing cybersecurity by imposing deadlines for certification of compliance and additional requirements for covered entities, Class A companies, and small businesses.

Under the amended regulation, material compliance now does not mean an absolute 100 percent compliance, but it does require that organizations subject to the NYDFS cybersecurity regulations take the appropriate action; it is a risk-based determination.

Mulrow-Peattie explained in the article that the "best interpretation is that whatever is wrong with the firm's cybersecurity program won't be enough to harm the covered firm in the event of a cybersecurity incident."

Covered firms are required to certify compliance with cybersecurity regulations for each of their affiliates separately. If an affiliate has a cybersecurity program that meets all relevant requirements, the covered firm can choose to adopt it either in full or in part. However, each covered entity remains responsible for its own compliance and annual certification.

What Deadlines Are Companies Facing Now?

- As of **December 1, 2023**, Covered Entities, Class A companies, and small businesses must report cyber incidents, including ransomware attacks, to NYDFS.
- On **April 15, 2024**, Covered Entities and Class A companies must submit an annual certification of compliance of their material compliance with the NYDFS cybersecurity regulations to the NYDFS.
- By **April 29, 2024**, Covered Entities and Class A companies are required to have in place revised cyber risk assessments informing revised cyber security policies to meet the new regulatory requirements.

Attorneys

Cathy Mulrow-Peattie

Service Areas

Privacy, Security & Artificial Intelligence

Offices

New York

The NYDFS has expanded the factors to be considered in evaluating risk beyond network hacking to reputational and customer risks.

Mulrow-Peattie added that "[p]art of the CISO's risk assessment should be an understanding of the risks to an organization's reputation and customers if there are insufficient cyber controls and a subsequent incident occurs." Noting that cybersecurity is a team sport, she recommended that covered firms include their finance, marketing, compliance, and legal teams when conducting a risk assessment.

The NYDFS and the SEC cyber incident reporting and disclosure requirements have different purposes; one is focused on cybersecurity compliance, and the other is focused on the disclosure of material information for investment decisions. "Regardless of the distinctions between the NYDFS and the SEC's rules, covered firms making any disclosures of cybersecurity events to both agencies should ensure that the information given to regulators is consistent," said Mulrow-Peattie.

Learn more about the updated NYDFS cybersecurity regulations in our recent *Privacy, Cyber & AI Decoded* alert.

"NY's New Cyber Law Shines Stronger Light on C-Level" was published by *FinOps Report* on February 11, 2024.