SECURITY BASECAMP

SBC Alert: NYDFS Amended Cybersecurity Regulation

NYDFS CYBERSECURITY REGULATION

On November 1, 2023, the New York Department of Financial Services (NYDFS) announced amendments to Cybersecurity Regulation, 23 NYCRR Part 500. The amended regulations aim to ensure cybersecurity risk is integrated into business planning, decision-making and ongoing risk management and include amendments to risk assessments, incident response and training.

JANUARY 2024

Security Basecamp
(949) 330-0899

Table of Contents

EXECUTIVE SUMMARY

On November 1, 2023, the New York Department of Financial Services (NYDFS) announced amendments to Cybersecurity Regulation, 23 NYCRR Part 500. The amended regulations aim to ensure cybersecurity risk is integrated into business planning, decision-making and ongoing risk management and include amendments to risk assessments, incident response and training. Updates to the regulation add strict provisions on board oversight of cybersecurity, ransomware payments, and event reporting. Covered entities have until April 29, 2024, to become compliant with these new amendments. However, changes to the reporting requirements go into effect earlier on December 1, 2023.

SELECTED UPDATES TO THE EXISTING REGULATION

The amendments include the following:

- Vulnerability Management: The expanded cybersecurity regulation includes additional requirements for vulnerability management practices in covered entities' cybersecurity policies. Beyond an annual risk assessment requirement, the updates to the rule also indicate that policies and procedures should be designed to ensure that covered entities conduct a penetration test (both internal and external to their systems) at least once a year.
- Cybersecurity Programs: The amendments set out new requirements for the maintenance of the cybersecurity programs of large companies (companies with at least $20M in gross annual revenue and over 2,000 employees). Cybersecurity programs for these entities will need to be audited annually based on a yearly risk assessment.
- Cybersecurity Governance: Amendments to the rule now require that covered entities designate a Chief Information Security Officer (CISO), employed by the covered entity, one of its affiliates, or a third-party service provider. CISOs will be required to report to senior governing bodies at least once a year regarding cybersecurity policies, issues, and risks. In addition, the most recent amendment to the regulation will require that the governing bodies or senior officers of each covered entity have "sufficient understanding of cybersecurity-related matters".
- Multi-Factor Authentication: Newly added to the existing rules are additional requirements for technology safety and access controls. Most notably, the amendments require covered entities to implement multi-factor authentication for any individual accessing any information systems, with some exceptions. Multi-factor authentication will be required for remote access to a covered entity's information systems, remote access to third-party applications, and to all privileged accounts.
- Cybersecurity Event Notice: The amendment also sets forth a strict reporting requirement that diverges from the recently passed U.S. Securities and Exchange Commission (SEC) standards for publicly traded companies. Rather than requiring companies to only report material incidents within a four-day timeline, the NYDFS now requires that covered entities make a report no less than 72 hours after determining that a cybersecurity event has occurred, regardless of materiality.
- Ransomware Payment Notification: In addition to the 72-hour reporting timeline for all cybersecurity events, the amendments set forth new reporting requirements in the event of a ransom payment made in connection with a cybersecurity event. Covered entities are required to provide notice of any such payments within 24 hours and will have 30 days to submit a full written reasoning behind making the payment, including alternatives considered before making the payment.
- Exemptions: The amendments expand the number of companies that qualify for small-company exemptions. Entities with fewer than 20 employees, less than $7.5M in gross revenue, or less than $15M in year-end total assets would be exempt from some of the cybersecurity requirements.

TRAINING RESOURCES

To help regulated entities plan for compliance, the Department has developed Part 500 training resources:

- Download the Cybersecurity Regulation Training Presentation (PDF)
- Watch the Cybersecurity Regulation Training Presentation (Video)

Additional videos, resources, and training opportunities will be posted to this section of the Cybersecurity Resource Center.

KEY COMPLIANCE DATES

The amended regulation's new compliance requirements will take effect in phases. Unless otherwise specified, covered entities have 180 days from date of adoption to come into compliance, or until April 29, 2024. Changes to reporting requirements take effect one month after publication of the amended regulation, or December 1, 2023. For certain other requirements, the regulation provides for up to one year, 18 months, or two years to come into compliance.

The below Cybersecurity Implementation Timelines outline key compliances dates for each of the categories of businesses impacted by the amended regulation:

- Implementation Timeline for Small Businesses
- Implementation Timeline for Class A Businesses
- Implementation Timeline for Covered Entities

ABOUT SECURITY BASECAMP

Security Basecamp (SBC) has highly experienced business-oriented cybersecurity professionals combining expertise across the breadth of financial service regulations, security frameworks, and information technology. Our mission is to help business-oriented entrepreneurs and senior managers know what they need to do to be cyber secure and compliant with applicable cybersecurity regulations. Much of the cybersecurity industry is built on selling complex solutions that are often difficult to understand. We aim to simplify that.

Collectively, our consultants have completed more than 300 cybersecurity risk assessments over the past eights years. We bring a business-oriented approach to completing cybersecurity projects and the technical acumen to work effectively with your internal IT staff. We help you manage cybersecurity analysis, action planning, and execution that your busy management team doesn't have the time or resources to lead. We offer three primary cybersecurity services: 1) Cybersecurity Risk Assessments, 2) CISO Support Services, and 3) Vendor Cybersecurity Due Diligence. To learn more, visit our website securitybasecamp.com or call (949) 330-0899.

AUTHOR INFORMATION

Paul Osterberg
Managing Director, Security Basecamp
(949) 330-0899
posterberg@securitybasecamp.com