THOMPSON HINE

Privacy & Cybersecurity Update

November 2023

NYDFS Amends Data Breach and Cybersecurity Regulations

On November 1, the New York Department of Financial Services (NYDFS) adopted a second amendment to its cybersecurity regulations (Amendment). These regulations focus on a broad range of issues, from data breach response to information governance to cybersecurity controls. The Amendment's requirements enter into force on a rolling basis, with changes to reporting requirements taking effect December 1, 2023, and other key obligations entering into force starting on April 29, 2024.

Ransomware, Extortion, and Data Breach Response

Pursuant to the Amendment, covered entities must notify NYDFS of a qualifying "cybersecurity incident" within 72 hours, whereas the previous regulation included notification requirements for "cybersecurity events."

The original NYDFS cybersecurity regulation defined a "cybersecurity event" as "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such information system." The Amendment creates a new term, "cybersecurity incident," which it defines as:

[A] cybersecurity event that has occurred at the covered entity, its affiliates, or a third-party service provider that: (1) impacts the covered entity and requires the covered entity to notify any government body, self-regulatory agency or any other supervisory body; (2) has a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity; or (3) results in the deployment of ransomware within a material part of the covered entity's information systems.

Accordingly, covered entities must report to the NYDFS certain cybersecurity incidents by which they are directly impacted and those impacting their affiliates or third-party service providers.

Further, each covered entity is required to "promptly" furnish the superintendent, upon request, with "any information" regarding the cybersecurity incident, and each has a "continuing obligation to update the superintendent with material changes or new information previously unavailable."

Moreover, in situations involving extortion payments, a covered entity must notify the superintendent within 24 hours of such payment being completed. Subsequently, within 30 days of the payment, a covered entity must submit to the superintendent a written description of why the payment was deemed necessary, any alternative measures considered, all efforts to find alternatives to such payment, and all diligence performed to ensure compliance with other applicable rules and regulations, including export control laws.

Incident Response and Business Continuity Planning

Each covered entity is required to implement and maintain a written incident response plan (IRP) that sets forth its proactive measures to investigate and mitigate cybersecurity events and ensure operational resilience, including but not limited to incident response, business continuity, and disaster recovery plans. The Amendment expands the content requirements so a covered entity must ensure its IRP now addresses its backup recovery process

and how it will prepare a root cause analysis that describes how and why the cybersecurity event occurred, what business impact it had, and what will be done to prevent reoccurrence.

The Amendment includes several business continuity and disaster recovery (BCDR) obligations. Specifically, a covered entity is required to adopt a BCDR plan that "shall be reasonably designed to ensure the availability and functionality of the covered entity's information systems and material services and protect the covered entity's personnel, assets and nonpublic information in the event of a cybersecurity-related disruption to its normal business activities." A BCDR plan must:

- Identify documents, data, facilities, infrastructure, services, personnel, and competencies essential to the continued operations of the covered entity's business.
- Identify the supervisory personnel responsible for implementing each aspect of the BCDR plan.
- Include a plan to communicate with essential persons in the event of a cybersecurity-related disruption to the covered entity's operations.
- Include procedures for the timely recovery of critical data and information systems and to resume operations as soon as reasonably possible following a cybersecurity-related disruption to normal business activities.
- Include procedures for backing up or copying, with sufficient frequency, information essential to the covered entity's operations and storing such information offsite.
- Identify third parties that are necessary to the continued operations of the covered entity's information systems.

Each covered entity shall periodically, but at least annually, test its IRP and BCDR plan with *all* staff and management critical to the response and revise the plans as necessary and test its ability to restore critical data and information systems from its backups.

Class A Companies and Cybersecurity Controls

The Amendment defines "Class A companies" as NYDFS-regulated businesses that either have over 2,000 employees or over $1 billion in gross annual revenue, in each case including the company's affiliates. A Class A company must conduct a "risk assessment" at least annually or whenever the business or technology causes a material change in cyber risk and design and conduct an independent audit of its cybersecurity program based on its risk assessment. It must implement a privileged access management solution as well as methods for automatically blocking commonly used passwords. It must also implement endpoint detection tools and other solutions to monitor and log potentially unauthorized activity.

The Amendment also sets forth additional cybersecurity controls applicable in certain circumstances, such as those related to encryption, vulnerability management (e.g., annual penetration and security testing and scanning), access management controls, and asset inventory.

The Amendment also requires a covered entity to implement multifactor authentication for individual access to any of its information systems. In the case of an exempt entity, multifactor authentication must be used for remote access to both its information systems and third-party applications, as well as all "privileged accounts other than service accounts that prohibit interactive login."

Greater Leadership Involvement

In addition to the annual report previously required under the regulation, a covered entity's chief information security officer (CISO) is now required to report to its senior governing body on material cybersecurity issues, including "significant cybersecurity events and significant changes to the covered entity's cybersecurity program."

Although the original regulation already required a covered entity's senior governing body to have sufficient knowledge or be advised by persons with sufficient expertise and knowledge to oversee cyber risk, the Amendment adds requirements that the senior governing body also provide oversight of and direction for the entity's cyber risk management program, including providing sufficient resources for program management.

Annual Notice

By April 15 of each year, a covered entity is required to provide the superintendent with one of the following:

- A written certification that the covered entity materially complied with its regulatory requirements during the prior calendar year. The certification must be based upon data and documentation sufficient to accurately determine and demonstrate such material compliance, including, to the extent necessary, documentation of officers, employees, representatives, outside vendors, and other individuals or entities, as well as other documentation, whether in the form of reports, certifications, schedules or otherwise.
- A written acknowledgment that (a) for the prior calendar year, the covered entity did not materially comply with all the requirements of the regulation; (b) identifies all sections of the regulation that the entity has not materially complied with and describes the nature and extent of such noncompliance; and (c) provides a remediation timeline or confirmation that remediation has been completed.

The certification or acknowledgment must be signed by the covered entity's highest-ranking executive and its CISO. If the covered entity does not have a CISO, the certification or acknowledgment must be signed by the highest-ranking executive and the senior officer responsible for the covered entity's cybersecurity program.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

Marla M. Izbicky
312.998.4253
Marla.Izbicky@ThompsonHine.com
Certified Information Privacy Professional/United States (CIPP/US)

Thora Knight
212.908.3971
Thora.Knight@ThompsonHine.com