NYS Department of Financial Services- Proposed Cybersecurity Requirements for Financial Services Companies

Establish a Cybersecurity Program – to establish a cybersecurity program based on a risk assessment designed to ensure the confidentiality, integrity and availability of information systems that performs five core cybersecurity functions:

- Identification of cyber risks.
- Implementation of policies and procedures to protect unauthorized access/use or other malicious acts.
- Detection of cybersecurity events.
- Responsiveness to identified or detected cybersecurity events to mitigate any negative events.
- Recovery from cybersecurity events and restoration of normal operations and services.
- Fulfillment of any applicable regulatory reporting obligations.

Also, see Additional Requirements.

Adopt a Cybersecurity Policy– be based on the Covered Entity's risk assessment and address the following areas to the extent applicable to the Covered Entity's operations:

- Information security.
- Data governance and classification.
- Access controls and identity management.
- Business continuity and disaster recovery planning and resources.
- Capacity and performance planning.
- Systems operations and availability concerns.
- Systems and network security.
- Systems and network monitoring.
- Systems and application development and quality assurance.
- Physical security and environmental controls.
- Customer data privacy.
- Vendor and third-party service provider management.
- Risk assessment.
- Incident response.

Additional Requirements – Each cybersecurity program must include:

- Annual penetration testing and vulnerability assessments.
- Implementation and maintenance of an audit trail system to reconstruct transactions and log access privileges.
- Limitations and periodic reviews of access privileges.
- Written application security procedures, guidelines, and standards that are reviewed and updated by the CISO at least annually.
- Periodic risk assessment to inform the design of the cybersecurity program and updated as needed of the confidentiality, integrity, and availability of information systems; adequacy of controls; and how identified risks will be mitigated or accepted.
    - The Covered Entity's risk assessment must allow for revision of controls to respond to technological developments and evolving threats and must consider the risks of the Covered Entity's business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems.
- The risk assessment must be carried out by written policies and procedures and must be documented. Such policies and procedures must include:
    - criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity;
    - criteria for the assessment of the confidentiality, integrity, security and availability of the Covered Entity's Information Systems and Nonpublic Information, including the adequacy of existing controls in the context of identified risks; and
    - requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.
- Employment and training of cybersecurity personnel to stay abreast of changing threats and countermeasures.
- Multi-factor authentication for individuals accessing internal systems who have privileged access or to support functions including remote access.
- Timely destruction of nonpublic information that is no longer necessary except where required to be retained by law or regulation.
- Monitoring of authorized users and cybersecurity awareness training for all personnel.
- Encryption of all nonpublic information held or transmitted.
    - For in transit data, this requirement is effective one year from the effective date of the regulation.
    - For at rest data, this requirement is effective five years from the effective date as long as there are compensating controls.
- Written incident response plan to promptly respond to, and recover from, any cybersecurity event materially affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations.

- **Designate Chief Information Security Officer (CISO)** – designate a qualified individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy. The CISO may be employed by the Covered Entity, one of its Affiliates or a Third Party Service Provider. To the extent this requirement is met using a Third Party Service Provider or an Affiliate, the Covered Entity will:
    - retain responsibility for compliance;
    - designate a senior member of the Covered Entity's personnel responsible for direction and oversight of the Third Party Service Provider; and
    - require the Third Party Service Provider to maintain a cybersecurity program that protects the Covered Entity.
- The CISO must report in writing at least annually to the Covered Entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report must be presented to a Senior Officer of the Covered Entity responsible for the Covered Entity's cybersecurity program. In preparing the report, the CISO will consider to the extent applicable:
    - the confidentiality of Nonpublic Information and the integrity and security of the Covered Entity's Information Systems;
    - the Covered Entity's cybersecurity policies and procedures;
    - material cyber risks to the Covered Entity;
    - overall effectiveness of the Covered Entity's cybersecurity program; and
    - material Cybersecurity Events involving the Covered Entity during the time period addressed by the report.

Third-Party Service Providers – must have policies and procedures designed to ensure the security of information systems and nonpublic information accessible to, or held by, third-parties and include the following:

- Identification and risk assessment of third-parties with access to such information systems or such nonpublic information.
- Minimum cybersecurity practices required to be met by such third-parties.
- Due diligence processes used to evaluate the adequacy of cybersecurity practices of such third-parties; and
- Periodic assessment, at least annually, of third-parties and the continued adequacy of their cybersecurity practices.

Click here for the full regulation.

Updated: December 2016