MARCH 08, 2024

Understanding New York Cybersecurity Requirements for Financial Services Companies

Every chief information security officer (CISO) and in-house lawyer responsible for data security legal issues should take an hour to read the New York State Department of Financial Services Cybersecurity Requirements for Financial Services Companies (23 NYCRR 500), which took effect March 1, 2017. Enforced by the superintendent of the department, these new regulations require regulated financial services companies—which are defined broadly under the law—to establish and maintain a fulsome cybersecurity program. The requirements provide an overview of what a strong cybersecurity program for any company, regardless of industry, should look like.

To whom do the regulations apply?

The regulations apply to covered entities, defined as any individual or nongovernmental entity operating under a license, registration, charter or similar authorization pursuant to New York's Banking, Insurance or Financial Services laws. Small financial services companies (those with fewer than 10 employees, less than $5 million in gross annual revenue and less than $10 million in year-end total assets) are exempt, as are financial services companies that do not operate or maintain any information systems or nonpublic information.

What needs to be achieved by August 28, 2017?

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:

Al Saikali
305.358.5171
asaikali@shb.com

Develop and maintain a cybersecurity program. The cybersecurity program must include core cybersecurity functions, such as (i) identifying and assessing internal and external cybersecurity risks; (ii) using defensive infrastructure and implementing policies and procedures to protect the covered entity's information systems and nonpublic information; (iii) detecting cybersecurity events; (iv) responding to identified cybersecurity events; and (v) fulfilling applicable regulatory reporting obligations.

The term "cybersecurity event" is defined broadly to include any attempt, including unsuccessful ones, to gain unauthorized access to an information system or information stored on such a system. The inclusion of unsuccessful attempts as a data security event is highly unusual for a data security law because it potentially opens the door to including the hundreds or thousands of phishing and other ordinary attempts that information security departments identify and filter out on a daily basis.

Notably, all documentation and information relevant to the covered entity's cybersecurity program must be made available to the superintendent of the Department of Financial Services. While the regulations exempt these records from public disclosure, all of this sensitive information could be compromised should the Department itself ever suffer a cyberattack. Imagine the damage attackers could do if they were able to learn the techniques and safeguards financial services companies use to protect sensitive information. It is hoped the Department of Financial Services will explain how it intends to safeguard this sensitive information shared by financial services companies.

Maintain a cybersecurity policy. Covered entities must implement and maintain a written cybersecurity policy setting forth the policies and procedures for protecting its nonpublic information and information systems.

Designate security personnel. This includes a CISO to oversee and implement the cybersecurity program and enforce the cybersecurity policy. The CISO may be employed by the covered entity or a third-party service provider. The CISO must report, in writing, annually to the covered entity's board of directors beginning March 1, 2018. The regulations describe with specificity what areas the report must address.

In addition, every covered entity must employ qualified cybersecurity personnel by August 28, 2017. These employees must manage cybersecurity risks and perform or oversee the performance of the core cybersecurity functions. The covered entity must train its personnel to ensure they are apprised of the latest relevant cybersecurity risks. The covered entity must also

Mayela Montenegro
949.975.1741
mmontenegro@shb.com

verify that their personnel take steps to maintain current knowledge of changing cybersecurity threats.

Implement access privileges. Each covered entity must limit user access privileges to information systems that provide access to nonpublic information. The covered entity must also periodically review such access privileges.

Develop an incident response plan. Every covered entity must develop a written incident response plan. The plan should address (i) the internal processes for responding to a cybersecurity event; (ii) the goals of the incident response plan; (iii) the definition of clear roles, responsibilities and levels of decision-making authority; (iv) external and internal communications and information sharing; (v) identification of requirements for the remediation of any identified weaknesses in information systems and associated controls; (vi) documentation and reporting regarding cybersecurity events and related incident response activities; and (vii) the evaluation and revision, as necessary, of the incident response plan following a cybersecurity event.

Notify the superintendent. Covered entities must notify the superintendent of the Department of Financial Services of a cybersecurity event within 72 hours of a determination that an event has occurred. The notification requirement, however, applies only to cybersecurity events in which either: (i) notice to any government body, self-regulatory agency or any other supervisory body is required; or (ii) there is a reasonable likelihood of materially harming any material part of the covered entity's normal operations.

Each year by February 15, the covered entity must submit to the superintendent a written statement certifying the covered entity was in compliance with the regulations during the prior calendar year. The statement must be signed by the chair of the board of directors or a similarly senior officer. The covered entity must keep supporting material for this statement for five years. If remediation, improvement, updating or redesign is necessary, the covered entity shall document the identification and remedial efforts planned or underway.

What needs to be achieved by March 1, 2018?

Risk assessment. Each covered entity must conduct a periodic risk assessment of its information system. The risk assessment must be carried out in accordance with written policies and procedures and must be documented. The policies and procedures must establish (i) criteria for the evaluation and categorization of

identified cybersecurity risks or threats facing the covered entity; (ii) the criteria for the assessment of the confidentiality, integrity, security and availability of the covered entity's information system and nonpublic information, including the adequacy of existing controls in the context of identified risks; (iii) requirements describing how identified risks will be mitigated or accepted; and (iv) how the cybersecurity program will address the risks. The assessment must be updated as necessary to address changes to the covered entity's information systems.

Multifactor authentication. Each covered entity must use effective controls to protect against unauthorized access to nonpublic information or information systems. Those controls may include multifactor authentication and risk-based authentication. Multifactor authentication means authentication through at least two of the following: (i) knowledge factors, such as passwords; (ii) possession factors, such as a text message on a mobile phone; or (iii) inherence factors, such as biometric characteristics. Multifactor authentication must be used by any individual accessing the covered entity's internal networks from an external network. Risk-based authentication means a system of authentication that detects anomalies or changes in the normal use patterns of a person that require additional verification of the person's identity when such deviations or changes are detected, such as the use of challenge questions.

CISO report. The covered entity's CISO must report on the cybersecurity program and material cybersecurity risks at least annually to the covered entity's board of directors or equivalent governing body or senior officer. The report may also address the confidentiality of nonpublic information, the covered entity's policies and procedures, the overall effectiveness of the cybersecurity program, and material cybersecurity events.

Penetration testing and vulnerability assessments. The covered entity must perform annual penetration testing of its information systems. Twice a year, it must also perform vulnerability assessments to identify publicly known cybersecurity vulnerabilities in the covered entity's information systems.

Training. The covered entity must provide regular cybersecurity awareness training for all personnel, updated to reflect risks identified by the covered entity in its periodic risk assessments.

What needs to be achieved by September 1, 2018?

Audit trail system. Each covered entity must securely maintain systems that are designed to reconstruct material financial

transactions to support normal operations and obligations (records must be kept for five years) and must include audit trails designed to detect and respond to cybersecurity events (records must be kept for three years).

Application security. Covered entities must prepare written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house applications developed and used by the company. Additionally, the company must develop procedures for evaluating, assessing or testing the security of externally developed applications it uses. These procedures, guidelines and standards must be periodically reviewed.

Limitations on data retention. Every covered entity must have policies and procedures for the secure disposal on a periodic basis of any nonpublic information that is no longer necessary for business operations or other legitimate business purposes.

Monitoring. The covered entity must implement risk-based policies, procedures and controls designed to monitor the activity of authorized users and detect unauthorized access to, use of or tampering with nonpublic information by such authorized users.

Encryption. Every covered entity should implement encryption of nonpublic information held or transmitted by the covered entity, both in transit over external networks and at rest. If encryption is unfeasible, the regulations allow for alternative compensating controls under certain circumstances.

What needs to be achieved by March 1, 2019?

Third-party service provider security policy. Every covered entity must implement written policies and procedures to ensure the security of nonpublic information and security systems that are accessible to, or held by, third-party service providers. These policies and procedures must address (i) the identification and risk assessment of the service providers; (ii) minimum cybersecurity practices required to be met by such providers; (iii) due diligence processes used to evaluate the adequacy of cybersecurity practices of such service providers; and (iv) periodic assessment of such service providers based on the risk they present and the continued adequacy of their cybersecurity practices. The policies must include guidelines for due diligence and contractual protections relating to service providers, including the provider's use of access controls, multifactor authentication, encryption, notice of a cybersecurity event, and representations and warranties addressing the provider's policies and procedures relating to security.

Conclusion

The regulations are useful for any company looking for ways to measure and improve its cybersecurity program. We contend that they will become the new standard for "reasonableness" by which the information security programs of companies will be judged in the future. They incorporate a strong mix of administrative, technical and physical safeguards that require periodic evaluation. Nevertheless, there are still open questions, and the Department of Financial Services may issue more guidance over time to provide answers. In the meantime, CISOs and in-house counsel looking for support from their respective organizations should consider using these regulations as a tool for that support.