CYBERSECURITY AND PRIVACY

NEW YORK MINIMUM CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

OVERVIEW AND REQUIREMENTS SUMMARY

HONIGMAN®

OVERVIEW

In response to increasing threats to information and financial systems, the New York State Department of Financial Services (DFS) recently finalized new cybersecurity regulations for financial institutions regulated by the DFS, which became effective on March 1, 2017. These new requirements impose minimum cybersecurity standards for adequately securing information and financial systems, as well as new cybersecurity event reporting and annual certification requirements.

Many larger institutions subject to DFS regulation will find compliance relatively straight forward. However, small and mid-sized covered entities should assess their cybersecurity program to determine how best to comply with these new requirements. Additionally, companies providing services to covered entities need to understand these new minimum requirements, as covered entities must now implement written policies and procedures to ensure the security of information systems and nonpublic information accessible to, or held by, service providers. The regulations include a staggered implementation timeline beginning 180 days from the effective date.

For entities not subject to the DFS regulation, the minimum cybersecurity requirements provide a useful roadmap for implementing or revising a cybersecurity program, particularly as other regulatory authorities and legislatures consider moving in a similar direction. In late March 2017, Colorado made the first such move by proposing new cybersecurity changes to the Colorado Security Act. Other state regulatory agencies may impose similar requirements in coming years, and companies looking to keep pace with evolving regulatory expectations can use the DFS minimum cybersecurity requirements as a helpful strategic planning guide.

1. What does the cybersecurity regulation require?

The Cybersecurity Requirements for Financial Services Companies regulation (23 NYCRR 500) requires covered entities to design and manage robust cybersecurity programs and processes. Under the regulation, covered entities must undertake tasks in several key areas:

- ***Cybersecurity Program Governance:*** Covered entities must establish a formal governance structure for managing cybersecurity efforts, including a designated program, written policies, dedicated personnel, appointment of a qualified chief information security officer and demonstrated senior management support.

- ***Administrative Processes:*** To support the cybersecurity program and regulatory compliance, covered entities need to implement several routine processes, including training programs, audit and compliance procedures and documentation, data retention practices and compliance certification.

- ***Risk Assessment and Management Activities:*** Covered entities must conduct risk assessments, supplemented with clear risk-mitigation strategies, and create a plan for identifying and responding to security incidents.

- ***Security Protocols:*** Cybersecurity programs must be supported by internal controls, including encryption, and covered entities must routinely test systems for vulnerabilities.

- ***Third-Party Oversight:*** Covered entities must create written policies and procedures to manage the risks associated with third-party providers, including due diligence protocols, contractual requirements and audit capabilities.

2. Who must comply with the cybersecurity regulations?

Entities currently regulated by the DFS must comply with the new regulation, including banks, insurance companies and other financial institutions. Exemptions are limited to entities:

- With fewer than 10 employees, including independent contractors;

- With less than $5M gross annual revenue for each of the last three years;

- With less than $10M year-end total assets (calculated by generally accepted accounting principles), including assets of all affiliates; or

- Acting as an employee, agent, representative or designee of a separate covered entity and subject to the other entity's cybersecurity program (if in compliance with the new regulation).

Additionally, covered entities that do not manage or control covered information must only comply with the risk assessment, third-party provider oversight and limitations on data retention requirements.

3. What information is subject to the cybersecurity regulations?

The regulation applies to all nonpublic information of a covered entity, which is more than nonpublic personal financial information, and is defined as:

- Nonpublic business information that if tampered with or disclosed, accessed, or used in any unauthorized manner could have a material adverse impact on the entity's business, operations or security;

- Nonpublic information that could identify an individual when in combination with that individual's social security number, drivers' license or identification card number, financial account numbers, access codes or passwords to financial accounts or biometric data; and

- Nonpublic information, except age and gender, created by or derived from a health care provider or an individual that relates to medical conditions, medical treatment, or payment for medical treatment.

4. When must companies be in full compliance with the cybersecurity regulation?

The regulation became effective on March 1, 2017, and covered entities have 180 days to comply with the new requirements. However, a few provisions have extended compliance deadlines.

180 DAY DEADLINE	12 MONTH DEADLINE	18 MONTH DEADLINE	24 MONTH DEADLINE
• Establish cybersecurity program • Create written cybersecurity policy • Appoint chief information security officer • Utilize additional personnel (if necessary) to support the cybersecurity program • Limit user access to nonpublic information • Create an incident response plan	• Provide written report on program and risks to board of directors/ senior management • Conduct penetration testing and vulnerability assessments • Assess risks of cybersecurity program and develop mitigation plans • Implement multifactor authentication • Provide regular cybersecurity training for all employees	• Ensure systems can create audit trails that can detect and respond to security events • Create written security procedures for developing internal applications and evaluating external applications • Define procedures to limit nonpublic information retention and manage secure disposal • Implement controls to monitor access activity • Implement encryption controls to protect held and transmitted data	• Implement a third-party provider security policy that clearly details processes for managing third-party risk, including due diligence, access controls, encryption and audit capabilities

5. How is the cybersecurity regulation enforced?

The DFS superintendent will enforce compliance with the regulation, and covered entities must submit annual certification of compliance with the requirements beginning February 15, 2018.

CYBERSECURITY PROGRAM GOVERNANCE*

CYBERSECURITY PROGRAM

Implement a cybersecurity program designed to protect information systems. The program must:

- Identify internal and external risks
- Implement a defensive structure for protecting information, including policies and procedures
- Detect and respond to cybersecurity events
- Recover from cybersecurity events and restore operations
- Fulfill regulatory obligations

REQUIRED ACTIVITIES

- Maintain documentation of the cybersecurity program and associated efforts

CYBERSECURITY POLICY

Create a written policy (or policies) detailing the company's approach to protecting information and systems. The policy, as applicable, should include the following areas:

- Information security
- Data governance and classification
- Asset inventory and device management
- Access controls and identity management
- Business continuity and disaster recovery planning and resources
- 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

REQUIRED ACTIVITIES

- Obtain senior management or board of director approval of the policy

CHIEF INFORMATION SECURITY OFFICER

Designate a qualified individual to serve as the chief information security officer (CISO) and manage the cybersecurity program.

REQUIRED ACTIVITIES

- Report on the cybersecurity program and associated risks to the board of directors (or a similar governing body) at least annually

CYBERSECURITY PERSONNEL AND INTELLIGENCE

Employ, as necessary, qualified cybersecurity personnel to support program operations and manage cybersecurity risks.

REQUIRED ACTIVITIES

- Provide cybersecurity updates and training to keep personnel informed on risks
- Ensure personnel engage in activities to maintain updated knowledge of cybersecurity risks

*Covered entities may be able to satisfy the cybersecurity program, chief information security officer, and cybersecurity personnel requirements if these resources are supplied by a third party or affiliate, provided the third party or affiliate practices can include the covered entity and meet the cybersecurity regulatory requirements.

ADMINISTRATIVE PROCESSES

TRAINING AND MONITORING	REQUIRED ACTIVITIES
Train employees regularly on cybersecurity risks and monitor employee use of systems to detect unauthorized use or tampering with information.	• Conduct regular cybersecurity awareness training • Implement policies and controls to monitor use of and access to information

AUDIT TRAIL	REQUIRED ACTIVITIES
Securely maintain systems, ensuring that systems can reconstruct financial transactions to support business operations and create audit trails to detect and respond to cybersecurity events.	• Maintain records for these activities for at least five years

LIMITATIONS ON DATA RETENTION	REQUIRED ACTIVITIES
Design procedures to ensure the routine destruction of information no longer necessary for business, legal or regulatory reasons.	• Delete obsolete data routinely and securely

NOTICES TO SUPERINTENDENT	REQUIRED ACTIVITIES
Certify compliance with the regulation to the DFS superintendent annually, including identified areas for compliance improvement and associated remedial efforts.	• Submit annual compliance certification no later than February 15 of each year (beginning 2018) • Maintain all documentation and data supporting certification for five years

EXEMPTIONS	REQUIRED ACTIVITIES
Submit a Notice of Exemption if the company qualifies under one of the exemption categories, indicating the exemptions that apply to the company.	• File Notice of Exemption with DFS • Comply with any regulatory provisions not excused by the exemption • Begin complying with all provisions of the regulation if (or when) the exemption ceases to apply

RISK ASSESSMENT AND MANAGEMENT ACTIVITIES

RISK ASSESSMENT	REQUIRED ACTIVITIES
Develop a process for conducting periodic risk assessments that identify cybersecurity risks and allow for updates to controls and processes designed to prevent risks. The written procedure should include: • Criteria for measuring and categorizing risks and threats • Criteria for assessing existing systems and information • Requirements for detailing mitigation steps or risk acceptance and how the cybersecurity program will address the risks	• Conduct periodic risk assessments • Update cybersecurity program and mitigation efforts based on risk assessment results • Document risk assessment activities

RISK ASSESSMENT AND MANAGEMENT ACTIVITIES *(continued)*

INCIDENT RESPONSE PLAN

Develop a written incident-response plan detailing the company's approach to responding to and recovering from a cybersecurity event. The plan must include:

- Processes for responding to a cybersecurity event
- Goals of the incident response plan
- Defined roles and responsibilities, including decision-making authority
- Plans for internal and external communications, as well as information sharing
- Procedures for remediating identified weaknesses
- Requirements for documenting and reporting the cybersecurity event and associated activities
- Processes for evaluating and revising the incident response plan following a cybersecurity event

REQUIRED ACTIVITIES

- Notify the DFS superintendent within 72 hours of detecting a cybersecurity event that requires notification or has a reasonable likelihood of harming normal operations

SECURITY PROTOCOLS

PENETRATION TESTING AND VULNERABILITY ASSESSMENTS

Engage in continuous monitoring or periodic testing of systems' vulnerabilities to assess the effectiveness of the cybersecurity program and associated controls.

REQUIRED ACTIVITIES

- Conduct annual penetration tests and biannual vulnerability assessments (if not engaged in continuous monitoring)

ACCESS PRIVILEGES

Limit access to systems containing nonpublic information.

REQUIRED ACTIVITIES

- Review access controls and access privileges periodically

APPLICATION SECURITY

Ensure internal development of applications includes security features and implement practices for evaluating the security capabilities of external applications.

REQUIRED ACTIVITIES

- Develop written procedures and guidelines for application development and review
- Review and update procedures periodically

MULTIFACTOR AUTHENTICATION

Implement controls to prevent unauthorized access to nonpublic information, using multifactor authentication when individuals access internal networks from an outside network.

REQUIRED ACTIVITIES

- Introduce multifactor authentication, or a reasonable equivalent approved by the CISO, for access from external networks

ENCRYPTION OF NONPUBLIC INFORMATION

Use encryption or an effective alternative control approved by the CISO to protect nonpublic information in transit over external networks or at rest.

REQUIRED ACTIVITIES

- Review controls and feasibility of encryption at least annually (if using alternative control)

THIRD-PARTY OVERSIGHT

THIRD-PARTY SERVICE PROVIDER SECURITY POLICY	REQUIRED ACTIVITIES
Design written policies for ensuring the security of systems and information made available to or held by third-party service providers and implement due diligence and contractual procedures for managing and evaluating third-party relationships. The policies should include: • Processes for evaluating third-party service provider risks • Requirements for minimum third-party security standards • Guidelines for conducting due diligence to evaluate third-party service provider security capabilities • Procedures for periodically assessing third parties and third-party cybersecurity practices Due diligence guidelines should include representations addressing third-party security practices and requirements for limiting access, using encryption and notifying of cybersecurity events.	• Manage oversight of third-party service provider security practices on an ongoing basis

CYBERSECURITY AND PRIVACY

MICHAEL P. HINDELANG CIPP/US, CIPM
313.465.7412
mhindelang@honigman.com

KARL A. HOCHKAMMER CIPP/US
313.465.7582
khochkammer@honigman.com