WHITE PAPER

The New York State Department of Financial Services New Cybersecurity Regulations Explained

Financial institutions in New York state have a new set of rules to live by.

Contained within Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York is a new compliance mandate requiring banks, insurers, and other financial institutions adopt additional layers of cybersecurity to protect their customers and their business. On March 1, 2017, the regulation, developed by the New York State Department of Financial Services (DFS), took effect. There is a grace period of sorts — organizations have 180 days from the day the regulations took effect to comply with most of the rules, and specific provisions have even later deadlines stretching out two years. Nevertheless, the countdown has begun, and starting Feb. 15, 2018, all organizations covered by the regulation will be required to annually prepare and submit a Certification of Compliance with the regulations to the DFS superintendent.

The new rules cover a significant amount of ground, including mandating wider use of multi-factor authentication and the encryption of all nonpublic data that is at rest or in transit. Implementing these changes may pose some challenges, but by understanding where your security posture as it relates to the regulation, you can begin to strategize what it will take to reach compliance or stay there. In this paper, we will examine the key parts of the regulations your organization needs to get a handle on.

The inability to identify and resolve advanced threats rapidly can result in publicity-generating breaches, business downtime, financial losses, and loss of competitive advantage.

Who Should Read This White Paper

- » CISO/CSOs
- » CIOs
- » CFOs
- » Directors of Security
- » Security Researchers
- » Security Architects

Beginning with the Basics

The regulation begins by requiring two items all organizations should already have — a cybersecurity program and policy. The cybersecurity program should:

- Identify internal and external threats
- Use defense infrastructure to protect the organization
- Detect, respond to, and recover from cybersecurity events
- Fulfill all regulatory reporting requirements

All documentation and information related to the program must be made available to the DFS superintendent upon request. In addition, each institution covered by the regulation is required to have a written cybersecurity policy approved by a senior officer or its board of directors. The policy must touch on several 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

The regulation also mandates organizations name a chief information security officer or its equivalent. This CISO will be responsible for "overseeing and implementing" the cybersecurity program and enforcing the cybersecurity policy. This CISO can be employed either by the organization, one of its affiliates or a third-party service provider. The CISO is also required to report in writing at least annually to the organization's board of directors or the equivalent governing body or person regarding the cybersecurity program and any material cybersecurity risks. In addition, organizations are required to build their own cybersecurity team or use a third-party service to protect their environment, as well as train and monitor the activities of authorized users.

By codifying what constitutes a sound cybersecurity program and policy, the regulation can help align your organization with industry best practices. If your cybersecurity policy and cybersecurity program do not involve all of the topics mentioned above, the first step in reaching compliance is to begin assessing your strategy towards those particular subjects.

Protecting Nonpublic Data

One of the provisions of the regulation likely to raise eyebrows is the requirement to encrypt "nonpublic data." There is a lengthy definition of what constitutes nonpublic data though boils down to this: it is any business-related information, which if disclosed, could have materially adverse impact on the business or person to whom it belongs. Some specifically cited examples include social security information, credit or debit card numbers, biometric records and health information.

Under the regulation, all financial organizations will have to implement encryption to protect nonpublic data in transit over external networks or at rest whenever feasible. If infeasible, the organization may secure information using compensating controls approved by the CISO. According to the rules, organizations have 18 months from March 1, 2017, to comply with this part of the regulation. Organizations should begin planning their encryption strategies now. Start by classifying the data that will need to be encrypted and determining where it is on the network. Then evaluate the different types of technologies available for what you need to accomplish, such as full disk encryption, email encryption, etc.

If the organization is using compensating controls such as network segmentation or database firewalls in lieu of encryption, be prepared to explain how these controls effectively meet the objective of the regulation.

Another critical part of protecting is building security into the application development lifecycle. The regulation mandates every organization have written procedures, guidelines and standards detailing secure development practices for in-house developed applications. There are a number of publically available resources to help you in this process, such as the Open Web Application Security Project (OWASP) and the CERT Division of the Software Engineering Institute.

In addition to applications developed internally, organizations must also have a documented process for assessing and testing the security of externally developed applications as well.

Understanding Your Security Posture

Just by assessing your organization's security posture, you have started down the path of compliance. The regulation mandates that organizations conduct periodic risk assessments. These assessments should be documented and updated as necessary to address changes to the IT environment. They should also include criteria for the evaluation and categorization of identified cybersecurity risks facing the organization; criteria for the assessment of the organization's information systems and nonpublic information; and requirements describing how risks will be mitigated or accepted and how the cybersecurity program will address the risks.

After identifying the data you want to protect, the next step is to identify threats to that data. The involves understanding how and where critical data is stored, who has access to it, and what security controls are in place to protect it and the resources on which it resides.

Putting the efficacy of those security controls to the test is important, and state regulators have recognized that. The regulation specifically requires vulnerability assessments and penetration tests in lieu of continuous monitoring that can detect any changes to systems that may create or indicate vulnerabilities. Penetration tests are to be conducted annually, and vulnerability assessments are required bi-annually. Organizations have one year to comply with both this part of the regulation as well as the risk assessment requirements. Third-party experts can help your organization with penetration tests and vulnerability assessments. Ensure that you properly define the scope of these tests so that the testers do not miss critical areas.

Staying secure also means knowing the security posture of third-party partners as well. Under the regulation, financial organization are expected to implement written policies and procedures designed to ensure the security of information systems and nonpublic information are accessible to or held by third-party service providers. Those policies should include the minimum-security practices the service provider must meet, as well as the processes used to evaluate the adequacy of their cybersecurity practices. In addition, the policy should include guidelines for contracts with providers.

Related to the issue of encryption is the subject of access control. The regulation specifically requires multifactor factor authentication be used to protect against unauthorized access to nonpublic information or systems. This includes any employees accessing the internal network from an external network. In addition, as part of their cybersecurity programs, financial organizations are required to limit and periodically review all user access privileges to information systems that provide access to nonpublic information.

Incident Response and Notification

Just as organizations should already have a written cybersecurity policy, they should also already have a written cyber-incident response plan. This plan must include: internal processes for responding to a cybersecurity event, definitions of roles and responsibilities, external and internal communication sharing plans, remediation requirements, documentation and reporting of cybersecurity events, and the evaluation and revision of the plan after a security event.

In addition, financial institutions are required to notify the DFS superintendent as promptly no later than 72 hours from the determination that a cybersecurity event has occurred. A cybersecurity event is defined as any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such a system. The superintendent only needs to be notified if the event has a reasonable likelihood of

affecting the organization's normal operations or if the organization is otherwise mandated to report it to any other governmental body or self-regulatory agency.

To comply with this part of the regulation, organizations should assess their incident response plans and ensure their procedures allow for prompt notification of cybersecurity events to DFS. Start with tabletop exercises. Remember, an incident response team should involve more than just IT — it should also involve legal, insurance, media relations and other important business decision makers and tailored towards your specific business risks.

Other Considerations

The regulation also has rules pertaining to data retention and auditing. Organizations have to maintain systems designed to reconstruct material financial transactions sufficient to support normal operations for at least five years, and include audit trails designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming the business for no less than three years.

Each organization must also 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. There is an exception for data that must be retained by law or regulation or if disposing of it is not reasonably feasible due to the manner in which the information is maintained.

What to Do

Meeting compliance mandates is not a new concept for financial institutions. It starts with understanding what the regulation is asking, and then moving on to figuring out how far your organization is from compliance.

- **Marshal your forces:** Brief your board of directors on the implications of the regulation on the business and develop an organized plan to approach the requirements.
- **Document what you do:** Make sure that your security policies and procedures and documented appropriately.
- **Determine your security posture**: Identify the data and systems that are critical to running your business and the security controls protecting them. Conduct a vulnerability assessment to assess your basic vulnerabilities, then a penetration test to test the efficacy of your security controls.
- **Reevaluate your cybersecurity incident response plan**: A plan on paper is just a plan on paper. You need to know if it is effective.

Identify where you are on the road to compliance, and determine how many steps it will take to get to where you need to be, and start your journey. The clock is ticking.

For more information, call **(877) 838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com