New York’s 23 NYCRR 500, a set of cybersecurity mandates and recommendations for the financial services industry, took effect on March 1, 2017. The law is the first of its kind in the United States and represents an early step in what may become a nationwide movement to improve data security through increased regulation.

The new regulations were issued by the New York State Department of Financial Services (DFS) and establish standards for security activities that, until now, have not been required by law. Covered organizations will be required to document their compliance in areas including cybersecurity risk assessment, penetration testing, data protection, and internal reporting. While the law applies specifically to organizations licensed by the New York DFS, it is likely to influence cybersecurity regulation in industries and jurisdictions across the country.

23 NYCRR 500 at a Glance

The New York DFS regulations were developed over several years, and were revised repeatedly in response to comments from financial firms and security experts. Rather than setting forth exact technical requirements, the law establishes general guidelines and minimum standards for information security. Some of the law’s key requirements are listed below.

- **Formal programs**: Covered organizations will be required to establish formal cybersecurity programs designed to identify cyber risks, protect data, detect attacks, and mitigate damage.

- **Written policies**: Organizations must document their cybersecurity policies and obtain approval for the policies from their senior officers or boards of directors.

- **CISO appointment**: Each covered entity will be required to appoint a Chief Information Security Officer, who will be responsible for implementing the organization’s cybersecurity program and enforcing its cybersecurity policy.

- **Risk assessments**: Organizations are expected to conduct regular risk assessments and revise their programs and policies as needed in response.
• **Application security:** Companies that develop their own software must define the procedures and standards they will follow to ensure the security of their applications.

• **Encryption:** Organizations should implement data protection methods including encryption to secure sensitive information they store or transmit.

• **Access control:** Organizations should use appropriate controls to limit access to sensitive information, including the use of multi-factor authentication for external users.

• **Notification:** Covered organizations must notify the New York DFS within 72 hours of a security breach or other cybersecurity event.

The regulations apply to a wide range of businesses, including banks, investment companies, insurance companies, brokerages, and mortgage companies. While the law’s definition of a covered entity may create confusion for some organizations (see “Open Questions” below), in general any business licensed by the New York DFS will need to comply with the law, regardless of where the business is headquartered.

Covered organizations will have between 180 days and two years to bring their cybersecurity practices into compliance with the law’s various provisions. Beginning in 2018, organizations covered by 23 NYCRR 500 will be required to provide a certificate of compliance to the New York DFS once per year, stating that they have met each of the law’s requirements.

## Rules for Third Party Service Providers

In addition to setting standards for covered entities themselves, 23 NYCRR 500 indirectly creates new obligations for third party service providers who are not licensed by the New York DFS.

Covered organizations are required to establish security policies for any of their third party providers who have access to nonpublic information. These third party policies must include many of the same general criteria that covered entities must use for their own policies:

• Risk assessments
• Access controls
• Notification of security events (to the covered entity in this case, rather than to the DFS)
• Use of encryption for sensitive information

In effect, even though they are not under the jurisdiction of the New York DFS, any service providers who wish to do business with a bank or other 23 NYCRR 500 covered entity will need to bring their own cybersecurity programs into compliance with the key provisions of the law.
Open Questions

Like most laws that address cybersecurity issues, 23 NYCRR 500 has created widespread confusion and uncertainty regarding its provisions. While many ambiguous elements were resolved with the final draft of the regulation, several key issues remain.

**Reporting requirements:** While the law states that organizations must report security events to the DFS, it does not give a specific definition of a security event, or set a threshold of severity that an event must reach in order to be reportable. Many companies have voiced concerns about the fact that unsuccessful attempts to access or misuse sensitive data are considered reportable under the new law. Unless some threshold is established, this requirement could create unmanageable burdens for large companies that defend themselves against hundreds or thousands of cyber attacks each day.

**Timing of risk assessments:** The law places a heavy emphasis on risk assessments, and states that cybersecurity programs and policies, access rules, encryption policies, authentication procedures, and many other required elements should all be based on an organization’s risk assessment. However, the requirement for conducting a risk assessment does not take effect until March 2018, while many items that depend on the assessment are required six months earlier.

**Definition of covered entities:** The law defines a covered entity as a business that is “…operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.” While most large financial institutions are clearly covered by the law (and some small businesses are specifically exempted), the wording is ambiguous enough to create confusion among many out-of-state organizations and service providers as to whether the law applies to them.

Similarities to the GDPR

While they are far less demanding and smaller in scope, the New York regulations share several similarities with the General Data Protection Regulation (GDPR) that will take effect in Europe in 2018.

- Both laws require covered entities to appoint high-level officers (a CISO in the New York law and a Data Protection Officer in the GDPR) who will take responsibility for cybersecurity operations and compliance.

- Both laws call for notification within 72 hours when an organization experiences a data breach. The GDPR, however, exempts an organization from this requirement if the compromised data is protected by strong encryption.

- Both laws require that organizations build security into their software from the beginning of the development process. The GDPR refers to this as “data protection by design” and “data protection by default.”

- Both laws specifically recommend the use of encryption to protect sensitive data at rest and in transit.

The similarities between 23 NYCRR 500 and the GDPR should simplify compliance for the large number of financial services organizations that operate in both Europe and New York, and will therefore be subject to both laws beginning in 2018.
Compliance Timeline

For most organizations, compliance with 23 NYCRR 500 will begin with an evaluation of the current cybersecurity program and the identification of any gaps between current practices and the new requirements. The regulations include four separate transitional periods, which can serve as a guide for the timing of compliance activities.

By August 2017
Starting from the new law’s effective date—March 1, 2017—covered organizations have 180 days to bring themselves into compliance with the first set of cybersecurity requirements:

- Create a cybersecurity program and define a cybersecurity policy
- Implement proper access controls for sensitive information
- Ensure that cybersecurity personnel are qualified and adequately trained
- Create an incident response plan and a process for notifying the DFS of security incidents

By March 2018
Within one year of the law’s effective date, organizations should be prepared to comply with a second set of requirements:

- Appoint a CISO
- Implement penetration tests, vulnerability assessments, and cybersecurity risk assessments
- Implement multi-factor authentication or equivalent controls for external access
- Provide cybersecurity awareness training to all personnel

By September 2018
Eighteen months after the effective date, some of the law’s more rigorous requirements take effect:

- Establish audit tracking for routine transactions and for security events
- Implement procedures to ensure the security of new applications
- Establish retention limits for sensitive information
- Implement activity monitoring for users with access to sensitive information
- Implement encryption or another strong form of data protection

By March 2019
A final requirement, calling for policies and procedures that govern third-party access to an organization’s sensitive information, takes effect two years from the initial effective date.

Compliance timelines will likely be accelerated for organizations that do business in Europe and must bring their data protection policies into compliance with the GDPR. In particular, organizations should pay special attention to the need for application security, strong encryption, and third-party access controls before the GDPR effective date of May 25, 2018.
Recommendations

Given the law’s lack of specific technological requirements, covered organizations will have a significant amount of freedom to determine how they will bring their security programs into compliance. The strategies listed below can help ensure that covered organizations not only satisfy the letter of the law, but make meaningful improvements to the security of their systems and data.

- **Use the NIST Cybersecurity Framework as a guide.** One common concern about the NY DFS regulations is that by prescribing certain actions and requiring an annual self-certification, the law will encourage a “check the box” mentality that may divert attention from an organization’s actual security needs. When developing or revising their programs, policies, and practices, organizations should refer to the National Institute of Standards and Technology (NIST) framework for guidance on best practices for planning and implementing a risk-based cybersecurity strategy. While it does not carry the force of law, the NIST framework can help organizations determine the best way to meet their compliance obligations and address their real-world issues.

- **Don’t delay a cyber risk assessment.** Even though the law does not technically require a cybersecurity risk assessment until 2018, every organization should be conducting regular assessments to identify existing and emerging vulnerabilities. Risk assessments should include an evaluation of asset vulnerabilities, documented threats, potential consequences of adverse events, and the likelihood that events will occur. A data discovery process, in which an organization locates and classifies the various forms of sensitive data in its possession, is an important first step in the risk assessment process.

- **Prepare for additional regulation.** Despite its limitations, 23 NYCRR 500 is expected to exert a strong influence on the future of cybersecurity legislation in the United States. As concerns about cyber threats continue to intensify, states across the country may follow New York’s lead and pass similar laws for the financial services sector, likely using the New York law as a reference point.

PKWARE’s Smartcrypt delivers strong encryption, simplified key management, and intelligent data discovery capabilities that can help your organization meet many of New York’s cybersecurity requirements. [Get the details in our 23 NYCRR 500 solution sheet, or contact us today to discuss your compliance and security needs.](#)

*PKWARE does not provide legal advice. While every effort has been made to ensure the accuracy of this material, this material has been prepared for informational purposes only, and is not intended to provide legal advice.*