FACT SHEET (Boldon James)

New York State Department Of Financial Services Cybersecurity Regulations

Protect Sensitive Data and Comply With 23 NYCRR 500

New York is one of the biggest financial hubs in the world; as you can imagine where there is sensitive financial information, there are people who want to get their hands on it. It is for this reason major financial firms operating in New York will face stiff cyber security obligations under the new regulations.

This regulation was put forward by the New York State Department of Financial Services (DFS) and will apply to firms holding a banking, insurance or financial services licence to operate in New York. 23 NYCRR 500 has been effective as of March 1st 2017, although firms have 180 days from this introduction date to change internal systems in order to meet new compliance and regulation standards.

A key area the new regulation looks to cover is the implementation of cybersecurity leadership throughout organisations by designating a qualified individual to serve as the CISO. This elected individual will be tasked with overseeing and enforcing the firm's cybersecurity program and policy. Each organisation will also need to implement regular staff training to cover specific cybersecurity risk areas.

The stipulations of the new regulation make sure organisations have detection, defence and response capabilities, including regulatory reporting as well as penetration testing. As with other new regulations, organisations must report any cyber security incidents to the DFS as promptly as possible (no later than 72 hours post incident).

Key Dates For Covered Entities

- **March 1, 2017** - Law becomes effective
- **August 28, 2017** - Must be compliant
- **September 27, 2017** - Deadline for filing Notices of Exemption Under 23 NYCRR 500.19(e)
- **February 15, 2018** - Deadline for covered entities to submit first certification under 23 NYCRR 500.17(b)
- **March 1, 2018** - One year transition period ends, must be in compliance with sections 500.04(b), 500.05, 500.09, 500.12, and 500.14(b)
- **September 3, 2018** - Eighteen month transition period ends, must be in compliance with sections 500.06, 500.08, 500.13, 500.14(a), and 500.15
- **March 1, 2019** - Two year transition period ends, must be in compliance with section 500.11

So how do organisations ensure they are compliant with 23 NYCRR 500? Evaluating the cybersecurity changes that may be required within the organisation with the senior management team - including the CISO and board of directors - is a good place to start. The key tasks organisations must complete to comply with 23 NYCRR 500 include:

- Appointment a CISO (if one isn't already in place)
- Perform risk assessments (which must be kept up to date on an ongoing basis)
- Document all organisational policies and procedures
- Perform penetration testing and vulnerability assessments
- Train all staff on a regular basis
- Monitor your assets and create audit trails
- Limit user privilege
- Securely destroy unnecessary data

Don't Delay Your Preparations

The sheer volume of unstructured data within organisations, combined with the ever increasing technical abilities hackers are using to breach perimeters, make it impossible to rely on people and processes alone to ensure that sensitive personal data is handled appropriately.

Data classification embeds a culture of compliance by involving users in identifying, managing and controlling regulated data, while automating parts of the protection process to enforce rules and policies consistently.

As you look at your organisations data protection policy, classifying data as a first step will enable the protection strategy and solutions you implement to be built around the types of data you have, and the levels of security they require.

How Can Boldon James Help?

Boldon James Classifier, the market leading data classification product, supports the creation and application of a data classification scheme by:

- Ensuring appropriate control of confidential or sensitive information
- Enforcing a classification and security policy consistently across the organisation
- Classifying or labelling data with visual (and metadata) labels to highlight any special handling requirements
- Alerting users when personal data is leaving the organisation to warn or prevent them from sending messages that contain sensitive information
- Educating users about the sensitivity of data whilst ensuring adherence to corporate policy
- Providing critical audit information on classification events to enable remediation activity and demonstrate compliance position to the DFS
- Utilising metadata labels to drive additional security controls and solutions, such as DLP, encryption and rights management

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.