logicworks

23 NYCRR 500 AND PUBLIC CLOUD

In the Fall of 2016, the New York State Department of Financial Services (DFS) announced a “first-in-the-nation regulation” to protect New York State from the threat of cyber attacks. The new cybersecurity regulations, known as Part 500 or 23 NYCRR 500, apply to any company licensed, accredited or authorized by New York’s Banking Law, Insurance Law, or Financial Services Law (with certain exemptions).

As a leading provider of public cloud services on AWS and Azure to financial services companies, Logicworks has received many questions about the new cybersecurity regulations — and we’ve answered them below.

23 NYCRR 500 AND PUBLIC CLOUD

WHEN DO I NEED TO BE IN COMPLIANCE WITH 23 NYCRR 500?

The law became effective March 1, 2017 and includes staggered periods for compliance as detailed in the graphic below. Companies must be prepared to submit a Certification of Compliance to DFS annually commencing February 15, 2018.

WHAT'S DIFFERENT ABOUT 23 NYCRR 500 FROM THE STANDARDS I ALREADY COMPLY WITH?

The financial services sector is already highly-regulated, so many of the requirements in the cyber-security regulations are covered by other regulations. Requirements like disaster recovery planning, audit trails, multi-factor authentication, and penetration testing should be familiar to IT teams that already operate systems in compliance with frameworks like PCI DSS 3.2 and GLBA.

Key additions from the cybersecurity regulations include:

- The requirement to designate a qualified Chief Information Security Officer ("CISO") for each Covered Entity who shall report in writing at least annually to the Covered Entity's board of directors or equivalent governing body (Section 500.4).
- The requirement to notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a security event occurred (Section 500.17).
- The requirement to perform an annual risk assessment (Section 500.09), to have senior management annual certify compliance (Section 500.00), and to securely destroy non-public information periodically (Section 500.13)

WHAT DOES 23 NYCRR 500 COVER?

You can find the full explanation of requirements here. In general, the cybersecurity regulations describe requirements relating to the following:

1. Establishment of a cybersecurity program with the following core cybersecurity functions:
    a. Ability to identify and assess internal and external cybersecurity risks that may threaten the security or integrity of your information systems;
    b. Ability to design and use defensive infrastructure and procedures to protect yoru information systems from unauthorized access;
    c. Ability to detect cybersecurity intrusions or breaches;
    d. Ability to respond to identified or detected cybersecurity events to mitigate any negative effects; and
    e. Ability to fulfill applicable regulatory reporting obligations.
2. Establishment of a cybersecurity policy based on your risk assessment that addresses areas such as:
    a. Information security
    b. Data governance and classification
    c. Access controls and identity management
    d. Business continuity and disaster recovery
    e. Capacity planning
    f. Systems operations and availability
    g. Systems and network security and monitoring
    h. Physical security and environmental controls
    i. Customer data privacy
    j. Incident response
3. Establishment of access controls
4. Training for employees
5. Assessment of third-party service provider risk
6. Incident monitoring and reporting
7. Multi-factor authentication
8. Encryption
9. Annual penetration testing and vulnerability assessments

WHAT ARE THE SPECIFIC REQUIREMENTS AROUND 3RD PARTY RISK MANAGEMENT?

In a report that the DFS published in 2015, they found that 95% of banking organizations conduct risk assessments with high-risk vendors. However, 21% of those surveyed do not require third parties to represent that they have established minimum information security requirements and only 36% of those extend requirements to fourth parties (subcontractors).

The requirement, set forth in Section 500.11, will not become effective until March 1, 2019. When effective, the requirements will include:

- Risk assessment of third party service providers
- Establishment of minimum cybersecurity practices to be met by a third party service provider. This includes policies to ensure that, where appropriate, the third party service providers use access controls, multi-factor authentication and encryption
- Due diligence to evaluate third party cybersecurity practices
- Periodic assessment of third party service provider

DO WE REALLY NEED A CISO?

The cybersecurity regulations do require that you designate a CISO. However, according to Section 500.04, “The CISO may be employed by the Covered Entity, one of its Affiliates or a Third Party Service Provider.” If you use a third party provider, a senior member of the Covered Entity’s personnel must oversee this person and be responsible for writing an annual report to the Covered Entity’s board of directors on the cybersecurity program and cybersecurity risks.

In some cases, Logicworks can serve as the third party CISO to support your compliance with the cybersecurity regulations.

WHAT IS THE CONTINUOUS MONITORING REQUIREMENT OF PART 500?

Each Covered Entity shall maintain records required by Audit Trail - Section 500.06(a)(1) of this Part for not fewer than five years and shall maintain records required by section 500.06(a)(2) of this Part for not fewer than three years.

Logicworks offers a tightly integrated 24x7x365 NOC / SOC with log retention options to help clients meet and exceed the Continuous Monitoring obligations of the regulation.

WHEN IS A COVERED ENTITY REQUIRED TO REPORT A CYBERSECURITY EVENT UNDER 23 NYCRR 500.17(A)?

23 NYCRR 500.17(a) requires Covered Entities to notify the superintendent of certain Cybersecurity Events as promptly as possible but in no event later than 72 hours from a determination that a reportable Cybersecurity Event has occurred. A Cybersecurity Event is reportable if:

- The Cybersecurity Event impacts the Covered Entity and notice of it is required to be provided to any government body, self-regulatory agency or any other supervisory body; or
- The Cybersecurity Event has a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

An attack on a Covered Entity may constitute a reportable Cybersecurity Event even if the attack is not successful.

WE WANT TO MIGRATE TO AWS OR ALREADY MANAGE SOME WORKLOADS ON AWS. HOW CAN WE MANAGE COMPLIANCE WITH THE CYBERSECURITY REGULATIONS IN AWS?

By migrating to AWS, customers have a shared compliance responsibility. This shared model means that AWS manages the infrastructure components from the host operating system (virtualization layer) down to the physical security of AWS' datacenters. It is the customer's responsibility to configure and secure AWS-provided services. In other words, AWS controls physical components; the customer owns and controls everything else. As AWS states repeatedly, "AWS manages security of the cloud, security in the cloud is the customer's responsibility." To learn more about managing compliance on AWS, download our free eBook.

In some ways, AWS can actually facilitate the process of implementing a robust cybersecurity program due to the availability of tools to automate certain controls.

The abstraction layer afforded by public cloud providers empowers a clear use of automation, often driven via Infrastructure as Code (IaC) and purposeful orchestration. The powerful result is that clients can perfectly define the intended state of every environment. By doing so, they accelerate their ability to deploy micro changes in addition to patches and configuration updates while understanding and mitigating many of the risks associated with change.

In Puppet's 2016 State of DevOps Survey, they found that high-performing IT teams recover from failure 24x faster than average IT teams.

HOW CAN LOGICWORKS HELP ME MEET 23 NYCRR 500 REQUIREMENTS?

Meeting new cybersecurity regulations -- and keeping up with changing requirements -- requires significant engineering time and talent. 48% of IT departments report that a lack of security skills is slowing down their cloud adoption plans, resulting in delayed projects and missed opportunities.

Logicworks helps companies build, operate, and secure public cloud environments that meet their specific regulatory requirements. Whether you are new to public cloud or already deployed on AWS or Azure, Logicworks can help you define security policies, support implementation of a mature cybersecurity program, and provide ongoing technical and security operations support for your cloud environment. This significantly reduces the burden on your engineering and cybersecurity teams and reduces the effort of maintaining compliance with regulations like 23 NYCRR 500.

Our services include:

- Discovery and technical assessment, including a security gap analysis using NIST 800-53 Risk Assessment Framework, AWS Well-Architected Framework, and 23 NYCRR 500
- Custom AWS. Azure, or Hybrid cloud design
- 24x7x365 Cloud management, monitoring, and technical support
- Access controls and identity management
- Installation and management of third party tools for intrusion detection, firewall, log retention and management, anti-virus, etc.
- Incident response
- Backups and Disaster Recovery
- Infrastructure automation services, including creation of infrastructure tempates to define consistent security configuration standards
- Access to Logicworks CISO to support your compliance with 23 NYCRR 500
- Access to Logicworks' Risk Assessment Reports
- For a complete list of our services, visit our website

Logicworks is a top provider of cloud services for financial services companies and a Leader in Gartner's 2017 Magic Quadrant for Public Cloud Managed Services Providers*. We work with companies like MassMutual and Janus Capital to provide IT management, automation, and security services. To learn more about our cloud services, please contact us or call (212) 625-5300.

logicworks

155 Avenue of the Americas, Fifth Floor | New York, NY 10013
P: 212.625.5300 | www.logicworks.com