DFS Compliance – Mandatory Cybersecurity Regulations

By:

Danielle V. Johnsen
Digital Edge Ventures, LLC
7 Teleport Drive
Staten Island, NY 10311
djohnsen@digitaledge.net
(718)-210-1698

June 2017

Executive Summary

On March 1, 2017, the New York State Department of Financial Services' (DFS) mandatory cybersecurity requirements for financial services entities became effective, with implementation to occur within 180 days (August 28, 2017). Thus, requiring banks, insurers, and other financial institutions to establish and maintain a "risk-based, holistic, and robust security program" that is ultimately designed to protect consumers' private data.

Why Use Digital Edge for your DFS Cyber Security Needs?

On Digital Edge Cybersecurity Team is well-versed in the DFS regulation. We are ready to help companies – and their boards of directors – both mitigate risk and ensure compliance with all aspects of the DFS regulation and best practices in cyber security including:

- **Third Party Assessment**
- **Policy Writing**
- Cyber & Security Alerting Appliance
- Physical Security and Environmental Controls
- Cyber Security Training & Refreshers
- Incident Response Plan
- Endpoint Security Suite
- Anti-Ransomware Protection w/Forensics
- Managed Firewall
- **Implementation of Security System**
- **Remote CISO (Chief Information Security Officer)**
- Asset Inventory and Device Management
- Third-Party Vendor Management
- Complete Set of Cyber & Business Policy Templates
- Compliance Deadline Reminders
- Web Security Suite
- Email & File Encryption
- Superintendent Notifications & Filings

About Us

Digital Edge provides unparalleled Managed Cloud Solutions, as well as, superior Information Technology Support Services. Skilled and accredited, with a proven track record for almost 20 years, we operate exclusively within prime data center facilities providing Enterprise IT Services expertise in:

- Managed Cloud Services
- Private and Hybrid Cloud
- Infrastructure as a Service
- IT Support and Outsourcing
- 24/7 NOC and SOC Operation
- Business Continuity and Disaster Recovery

Digital Edge's organization is nicely balanced between our experience and ability to support a number of Enterprise Class IT organizations with complex needs and large processing demands, while staying quick and flexible.

Internally, the Digital Edge team strives to deliver any solution with **Stability, Security, Efficiency** and **Compliance.** This is the heart beat of Digital Edge. We achieve this drive through years of experience in engineering solutions, high level of IT management automation and constant innovation.

Getting Ready For New York DFS Cybersecurity Regulation

On March 1, 2017, the New York State Department of Financial Services' (DFS) mandatory cybersecurity requirements for financial services entities became effective, with implementation to occur within 180 days (August 28, 2017). Thus, requiring banks, insurers, and other financial institutions to establish and maintain a "risk-based, holistic, and robust security program" that is ultimately designed to protect consumers' private data.

This act is the first-in-the-nation cyber security regulation for financial institutions, and the requirements from DFS go beyond what we've historically seen from regulators. Banks, insurance companies, and companies that do business in New York must now assess their cyber risks, implement a comprehensive, written cybersecurity program, as well as manage the cyber risks of their third-party vendors. This groundbreaking regulation now holds company board members **personally liable** for annual compliance certification.

At a high level, the regulation requires that all covered entities:

- Conduct a documented risk assessment
- Establish a risk-based cybersecurity program
- Adopt a written cybersecurity policy
- Designate a qualified CISO
- Implement written third-party cyber risk policies
- Establish a written incident response plan
- Notify the superintendent of DFS of any cybersecurity events
- Submit an annual certification of compliance

Accordingly, this regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization's cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity's cybersecurity program must ensure the safety and soundness of the institution and protect its customers.

(For more information regarding the DFS Cybersecurity Regulation 23 NYCRR Part 500, please view the Appendix.)

Why Now?

DFS has been closely monitoring the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors. Recently, cybercriminals have sought to exploit technological vulnerabilities to gain access to sensitive electronic data. Cybercriminals can cause significant financial losses for DFS regulated entities as well as for New York consumers whose private information may be revealed and/or stolen for illicit purposes. The financial services industry is a significant target of cybersecurity threats. DFS appreciates that many firms have proactively increased their cybersecurity programs with great success.

Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances.

It is critical for all regulated institutions that have not yet done so to move swiftly and urgently to adopt a cybersecurity program and for all regulated entities to be subject to minimum standards with respect to their programs. The number of cyber events has been steadily increasing and estimates of potential risk to our financial services industry are stark. Adoption of the program outlined in these regulations is a priority for New York State.

Key Dates: DFS's Cybersecurity Regulation (23 NYCRR Part 500)

March 1, 2017 - 23 NYCRR Part 500 becomes effective.

August 28, 2017 - 180-day transitional period ends. Covered Entities are required to be in compliance with requirements of 23 NYCRR Part 500 unless otherwise specified.

September 27, 2017 – Initial 30-day period for filing Notices of Exemption under 23 NYCRR 500.19(e) ends. Covered Entities that have determined that they qualify for a limited exemption under 23 NYCRR 500.19(a)-(d) as of August 28, 2017 are required to file a Notice of Exemption on or prior to this date.

February 15, 2018 - Covered Entities are required to submit the first certification under 23 NYCRR 500.17(b) on or prior to this date.

March 1, 2018 - One year transitional period ends. Covered Entities are required to be in compliance with the requirements of sections 500.04(b), 500.05, 500.09, 500.12 and 500.14(b) of 23 NYCRR Part 500.

September 3, 2018 - Eighteen-month transitional period ends. Covered Entities are required to be in compliance with the requirements of sections 500.06, 500.08, 500.13, 500.14(a) and 500.15 of 23 NYCRR Part 500.

March 1, 2019 - Two-year transitional period ends. Covered Entities are required to be in compliance with the requirements of 23 NYCRR 500.11.

Is Your Business Prepared to Meet These Requirements?

It is critical for all regulated institutions that have not yet done so to move swiftly and urgently to adopt a cybersecurity program and for all regulated entities to be subject to minimum standards with respect to their programs. The number of cyber events has been steadily increasing and estimates of potential risk.

Let the Digital Edge Cyber Security Team ease the burden of implementing the robust NYDFS Cybersecurity Regulation. Contact our Sales Team at for your free assessment and align yourself with compliance today!

Appendix: NYDFS's Cybersecurity Regulation (23 NYCRR Part 500)

Section 500.03 Cybersecurity Policy

Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations:

(a) information security;
(b) data governance and classification;
(c) asset inventory and device management;
(d) access controls and identity management;
(e) business continuity and disaster recovery planning and resources;
(f) systems operations and availability concerns;
(g) systems and network security;
(h) systems and network monitoring;
(i) systems and application development and quality assurance;
(j) physical security and environmental controls;
(k) customer data privacy;
(l) vendor and Third-Party Service Provider management;
(m) risk assessment; and
(n) incident response.

Section 500.04 Chief Information Security Officer

Each Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy. The CISO may be employed by the Covered Entity, one of its Affiliates or a Third Party Service Provider. To the extent this requirement is met using a Third Party Service Provider or an Affiliate, the Covered Entity shall:

(1) retain responsibility for compliance with this Part;
(2) designate a senior member of the Covered Entity's personnel responsible for direction and oversight of the Third Party Service Provider; and
(3) require the Third Party Service Provider to maintain a cybersecurity program that protects the Covered Entity in accordance with the requirements of this Part.

The CISO of each Covered Entity shall report in writing at least annually to the Covered Entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a Senior Officer of the Covered Entity responsible for the Covered Entity's cybersecurity program. The CISO shall report on the Covered Entity's cybersecurity program and material cybersecurity risks. The CISO shall consider to the extent applicable:

(1) the confidentiality of Nonpublic Information and the integrity and security of the Covered Entity's Information Systems;
(2) the Covered Entity's cybersecurity policies and procedures;
(3) material cybersecurity risks to the Covered Entity;
(4) overall effectiveness of the Covered Entity's cybersecurity program; and
(5) material Cybersecurity Events involving the Covered Entity during the time period addressed by the report.

Section 500.05 Penetration Testing and Vulnerability Assessments

The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity's Risk Assessment, designed to assess the effectiveness of the Covered Entity's cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic Penetration Testing and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct:

(a) annual Penetration Testing of the Covered Entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and
(b) bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems based on the Risk Assessment.

Section 500.06 Audit Trail

Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment:

(1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and
(2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.

Each Covered Entity shall maintain records required by 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.

Section 500.07 Access Privileges

As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.

Section 500.08 Application Security

Each Covered Entity's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment.

All such procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the Covered Entity.

Section 500.09 Risk Assessment

Each Covered Entity shall conduct a periodic Risk Assessment of the Covered Entity's Information Systems sufficient to inform the design of the cybersecurity program as required by this Part. Such Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems,

Nonpublic Information or business operations. The Covered Entity's Risk Assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the Covered Entity's business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems.

The Risk Assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include:

(1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity;
(2) criteria for the assessment of the confidentiality, integrity, security and availability of the Covered Entity's Information Systems and Nonpublic Information, including the adequacy of existing controls in the context of identified risks; and
(3) requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.

Section 500.10 Cybersecurity Personnel and Intelligence

In addition to the requirements set forth in section 500.04(a) of this Part, each Covered Entity shall:

(1) utilize qualified cybersecurity personnel of the Covered Entity, an Affiliate or a Third Party Service Provider sufficient to manage the Covered Entity's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in section 500.02(b)(1)-(6) of this Part;
(2) provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks; and
(3) verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

A Covered Entity may choose to utilize an Affiliate or qualified Third Party Service Provider to assist in complying with the requirements set forth in this Part, subject to the requirements set forth in section 500.11 of this Part.

Section 500.11 Third Party Service Provider Security Policy

Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address to the extent applicable:

(1) the identification and risk assessment of Third Party Service Providers;
(2) minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity;
(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers; and
(4) periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers including to the extent applicable guidelines addressing:

(1) the Third Party Service Provider's policies and procedures for access controls, including its use of Multi-Factor Authentication as required by section 500.12 of this Part, to limit access to relevant Information Systems and Nonpublic Information;
(2) the Third Party Service Provider's policies and procedures for use of encryption as required by section 500.15 of this Part to protect Nonpublic Information in transit and at rest;

(3) notice to be provided to the Covered Entity in the event of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or the Covered Entity's Nonpublic Information being held by the Third Party Service Provider; and
(4) representations and warranties addressing the Third Party Service Provider's cybersecurity policies and procedures that relate to the security of the Covered Entity's Information Systems or Nonpublic Information.

Section 500.12 Multi-Factor Authentication

Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.
Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.

Section 500.13 Limitations on Data Retention

As part of its cybersecurity program, each Covered Entity shall include policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information identified in section 500.01(g)(2)-(3) of this Part that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Section 500.14 Training and Monitoring

As part of its cybersecurity program, each Covered Entity shall:
(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users; and
(b) provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.

Section 500.15 Encryption of Nonpublic Information

As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.

To the extent a Covered Entity determines that encryption of Nonpublic Information in transit over external networks is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

To the extent a Covered Entity determines that encryption of Nonpublic Information at rest is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

To the extent that a Covered Entity is utilizing compensating controls under (a) above, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.

Section 500.16 Incident Response Plan

As part of its cybersecurity program, each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations.

Such incident response plan shall address the following areas:
(1) the internal processes for responding to a Cybersecurity Event;
(2) the goals of the incident response plan;
(3) the definition of clear roles, responsibilities and levels of decision-making authority;
(4) external and internal communications and information sharing;
(5) identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;
(6) documentation and reporting regarding Cybersecurity Events and related incident response activities; and
(7) the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

Section 500.17 Notices to Superintendent

Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following:

(1) Cybersecurity Events impacting the Covered Entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or
(2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

Section 500.18 Confidentiality

Information provided by a Covered Entity pursuant to this Part is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable state or federal law.

Section 500.19 Exemptions

Limited Exemption. Each Covered Entity with:

(1) fewer than 10 employees, including any independent contractors, of the Covered Entity or its Affiliates located in New York or responsible for business of the Covered Entity, or
(2) less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the Covered Entity and its Affiliates, or
(3) less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates,
shall be exempt from the requirements of sections 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

An employee, agent, representative or designee of a Covered Entity, who is itself a Covered Entity, is exempt from this Part and need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the Covered Entity.

A Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

A Covered Entity under Article 70 of the Insurance Law that does not and is not required to directly or indirectly control, own, access, generate, receive or possess Nonpublic Information other than information relating to its corporate parent company (or Affiliates) shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

A Covered Entity that qualifies for any of the above exemptions pursuant to this section shall file a Notice of Exemption in the form set forth as Appendix B within 30 days of the determination that the Covered Entity is exempt.

The following Persons are exempt from the requirements of this Part, provided such Persons do not otherwise qualify as a Covered Entity for purposes of this Part: Persons subject to Insurance Law section 1110; Persons subject to Insurance Law section 5904; and any accredited reinsurer or certified reinsurer that has been accredited or certified pursuant to 11 NYCRR 125.

In the event that a Covered Entity, as of its most recent fiscal year end, ceases to qualify for an exemption, such Covered Entity shall have 180 days from such fiscal year end to comply with all applicable requirements of this Part.

Section 500.20 Enforcement

This regulation will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent's authority under any applicable laws.