WAVESTONE

HOW NEW YORK CYBER-REGULATION IS CHANGING THE FINANCIAL INDUSTRY?

NYS DFS REGULATION 23 NYCRR 500

The regulation, first of its kind, lays out detailed cybersecurity requirements for financial services firms within the jurisdiction of the NYS DFS. This publication provides the summary of the NYS DFS cybersecurity priorities and timeline constraints and highlights how to leverage past initiatives such as FFIEC CAT in the Financial Institution's compliance process.

AUTHORS

NICOLE SHU
nicole.shu@wavestone.com

CYRIL KORENBEUSSER
cyril.korenbeusser@wavestone.com

This study was carried out with the help of Caleb Ferguson and Kevin Zhang

1/ THE NYS DFS CYBER REGULATION IS LIVE

In September 2016, the New York State Department of Financial Services (NYS DFS) broke ground as the first state to publish a regulation ("23 NYCRR 500") on the cybersecurity of banks, insurance companies, and other financial institutions operating in New York, including internal and external services providers and foreign banking institutions (FBOs) with branches in New York.

The regulation was proposed following the survey of two hundred regulated institutions (Banks and Insurers) and then revised based on feedback received during subsequent periods for public comment. It took effect on March 1st, 2017, and mandates that regulated institutions submit their first certifications of compliance by February 18th, 2018.

> « As our global financial network becomes even more interconnected and entities around the world increasingly suffer information breaches, New York is leading the charge to combat the ever-increasing risk of cyber-attacks. »
>
> NYS-DFS Superintendent Maria T. Vullo

Current timeline of the 23 NYCRR 500

› REGULATION FIRST PUBLICATION:	09/13/16
› UPDATED VERSION:	12/28/16
› FINAL VERSION:	02/16/17
› **EFFECTIVE DATE:**	**03/01/17**
› **1ST CERTIFICATION SUBMISSION DATE:**	**02/15/18**

The regulation is intended to ensure that financial institutions regulated by the NYS DFS implement and maintain a cybersecurity program to protect consumers and New York's financial services industry as a whole. It aims to prevent disruption of services and other harmful consequences of cyber-attacks through protection of institutions' information systems and the nonpublic information (NPI) stored on those systems.

2/ COMPLIANCE WITH THE REGULATION IS REQUIRED, AND AUDITS ARE EXPECTED TO START SOON

By the first certification submission date, financial institutions must assess their specific risk profiles (including the risks derived from their activities, businesses, and third parties) and build an appropriate cybersecurity program with corresponding policies. The regulation touches on all aspects of cybersecurity, including responsibilities of the CISO, cyber-awareness among all staff, third party security, appropriate risk controls, and enterprise resilience against cyber issues. While the risk assessment will inform the program, it will also help the CISO obtain an immediate understanding of the cybersecurity capabilities within their institution.

Inputs and results of cybersecurity office working towards NYS DFS compliance

However, between now and 2018, financial institutions have a milestone to meet. By August 28th, covered entities must comply with challenging risk assessment requirements and risk-based cybersecurity control requirements. These requirements include performing an initial assessment of threats and business risks within the enterprise, identifying underlying assets and vulnerabilities that impact business priorities in case of a cyber incident, as well as developing an operating model to remediate control gaps discovered in the assessment.

Key activities due by August 28th, 2017

What needs to be done

OPERATING MODEL FOR CYBER RISK MANAGEMENT	THREAT & RISK ASSESSMENT	IDENTIFICATION OF UNDERLYING ASSETS	VULNERABILITIES ASSESSMENT
Develop the cyber risk assessment organization, governance and processes	Identify top priority cyber threats and risks by business line and function	Identify and map risk to each key asset (data and systems)	Evalate systems' security weaknesses through penetration testing

3/ BEYOND THE CURRENT DUE-DATES, MORE PREPARATION IS NEEDED

While completing the early requirements from the NYS DFS, financial institutions will find they are faced with 3 main challenges that are at the heart of the NYS DFS mandate:

Recurrent, central challenges presented by 23 NYCRR 500

RISK - DRIVEN CYBERSECURITY PROGRAM

/ Consider risk for business operation
/ Consider underlying data and systems
/ Consider controls availability and effectiveness
/ Rely on a comprehensive risk management framework

PROTECTING NONPUBLIC INFORMATION

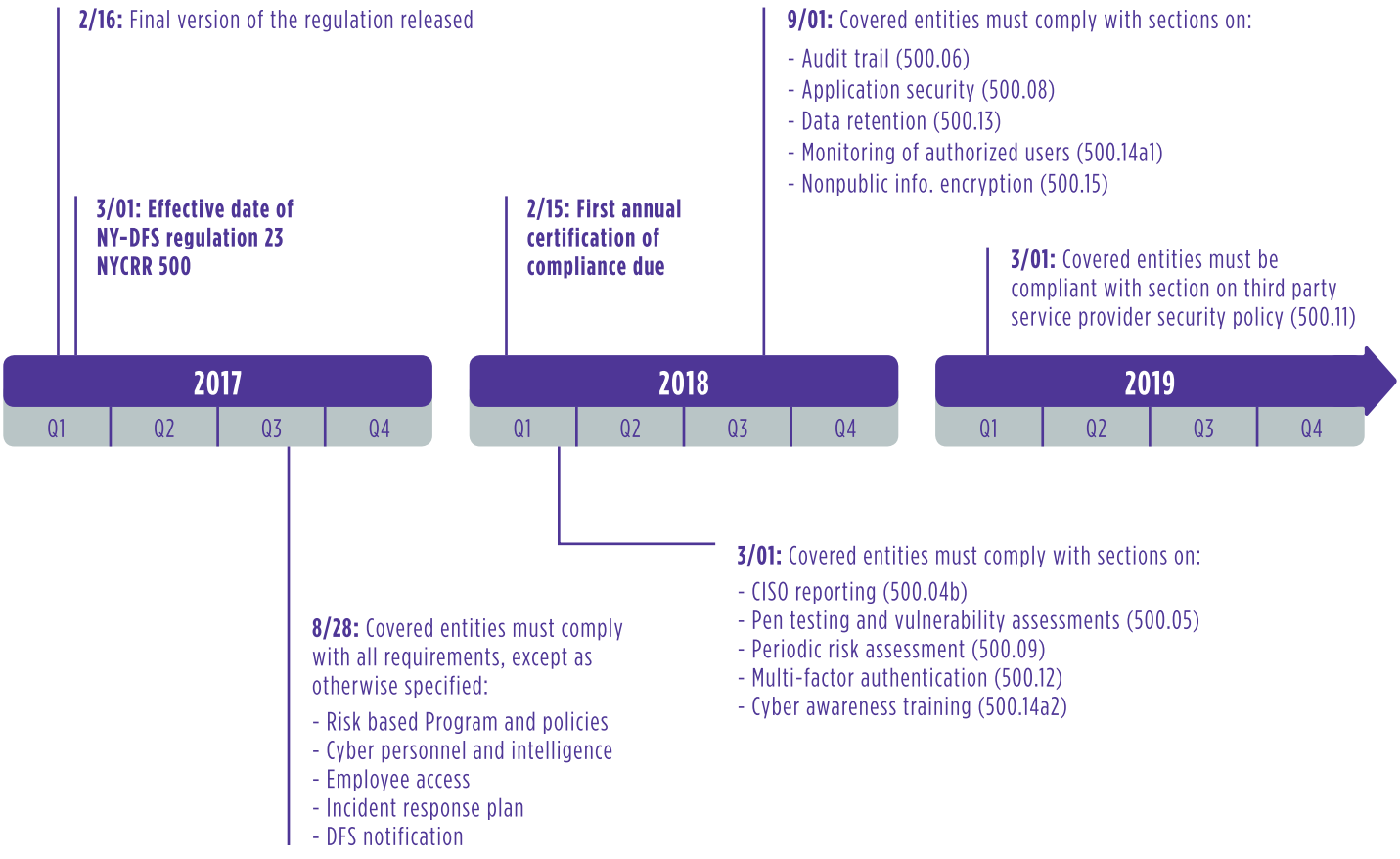
/ Limit user access privilege
/ Develop multi-factor authentication
/ Monitor access and activity
/ Encrypt data
/ Develop secure disposal procedures

EMPOWERING THE CISO

/ Report to Senior Management on the program and material risks
/ Implement and oversee a risk based cybersecurity program
/ Implement and maintain cybersecurity policies

These challenges will require constant attention as financial institutions and their CISOs prepare a plan to deliver on each of the milestone mandated by the NYS DFS through 2019.

Schedule for compliance with NYS DFS



4/ PRIORITY CONTROL AREAS FOR REMEDIATION

Certain regulatory requirements within NYS DFS 23 NYCRR 500 can be prioritized due to either their significance in remediating potential risks or the challenge of their implementation. Prioritized requirements include:

/ Risk based program and policies

It comes as no surprise that 'risk-based program and policies' is included in this first set of requirements due to NYS DFS. Adjusting cyber programs and policies to a risk-based model is a key priority, as it will shape and drive how financial institutions develop and manage their other cyber capabilities.

It is also poised to be one of the biggest challenges for banks to face, as it calls for participation from stakeholders across the organization, forces the CISO to consider and make decisions regarding many cyber security topics, and requires formal acknowledgment and approval from senior management.

/ Periodic risk assessment

A period risk assessment is required in order to challenge and test the design of the institution's cybersecurity program. The risk assessment is of highest priority because of its role in identifying potential risks and gaps for remediation. From a risk-based perspective, the risk assessment enables institutions to categorize their risks and prioritize control remediation.

/ Audit trail

Firms are required to maintain systems that can reconstruct material financial transactions for at least five years into the past.

/ Data retention

Document retention policies must be modified to retain documents for at least five years. However, firms need to facilitate periodic disposals of NPI that is no longer necessary for business operations.

/ Protecting nonpublic information

The regulation requires that firms implement encryption controls on NPI in transit over external networks and at rest. To do this properly, firms must first be able to classify their data in order to identify all of the NPI they possess. This may pose a challenge depending on the current network architecture of the firm. The regulation also requires that firms implement continuous monitoring controls that identify unauthorized access or use of NPI.

/ Cyber awareness training

Distribute cybersecurity awareness training to all personnel and update based on identified risks. Awareness is a priority because of its role in preventing non-malicious insider threats.

/ Third party service provider security policy

Firms must implement policies and procedures that secure the information systems and NPI held by third parties. Depending on the maturity of the firm's existing third party management policies, it may be a significant challenge to create and apply the necessary changes.

5/ EXISTING CYBERSECURITY FRAMEWORKS ARE A GOOD STARTING POINT, BUT NOT ENOUGH

When making the effort comply with the new regulation, it is important to know that the NYS-DFS regulation has areas of focus beyond the requirement of current cybersecurity guidelines, such as the FFIEC Cybersecurity assessment or FFIEC CAT, address. Such requirements include:

/ **Board and senior management responsibilities**
- › Designation of an individual responsible as the CISO
- › Detailed description of CISO responsibilities
- › Involvement of the board in the program strategy/validation

/ **Risk based program**
- › Assessment of entities' risks (business, operation, technology) with periodic update
- › Scope covering Integrity, Availability and Confidentiality

THE REGULATION IS NOT INTENDED TO BE PRESCRIPTIVE BUT RATHER ESTABLISH BASELINE CYBERSECURITY STANDARDS FOR FINANCIAL INSTITUTIONS. Other frameworks such as the FFIEC CAT provide details on procedures, and capabilities (e.g., infrastructure management, incident escalation) that could be developed.

/ **Third parties**
- › Cyber-program to be extended to the 3rd parties
- › Preventive controls applicable to the 3rd party including multifactor authentication and encryption

/ **Information system testing**
- › Definition of the frequency: annual penetration testing and biannual vulnerability assessments if effective continuous monitoring is non-existent

/ **Nonpublic information (NPI)**
- › Stronger emphasis on encryption of NPI in transit and at rest
- › Strict controls on systems managing NPI
- › Continuous monitoring of access to NPI

/ **Audit trail**
- › Maintenance of cyber-records for at least five years
- › Ability to reconstruct material financial transaction (operation and regulation)

/ **DFS communication**
- › Notification of certain cyber events within 72 hours
- › Annual certification of compliance submitted by Board/Senior Officer

Institutions will need to identify and resolve the gaps between their current cybersecurity programs and regulatory requirements within NYS-DFS NYS DFS 23 NYCRR 500 in order to maintain good standing with the regulators.

CONCLUSION

NYS-DFS regulation, first of its kind in the US, lays out the mandatory cyber-foundations expected for any financial firm with a detailed list of cybersecurity requirements. Beyond the technical capabilities to be developed there is 4 major requirements that would impact the organization and could be summarized as:

1. Focusing on an enterprise risk-driven cybersecurity program;
2. Protecting non-public information (NPI);
3. Empowering the CISO role and responsibilities;
4. And claiming the ownership of the program up to the board of directors.

Existing cybersecurity guidance and frameworks such as FFIEC CAT & handbooks, NIST CSF, or ISO 2700x propose structures to organize and manage either controls, capabilities and cyber-maturity. However, NYS-DFS remains, in its latest version, not too prescriptive and introduce the components of what we call a risk-top-down approach with results assessment. The regulator started answering the difficult question of the territoriality of the requirements, clarifying the collaboration between US CISOs and their worldwide counterparties.

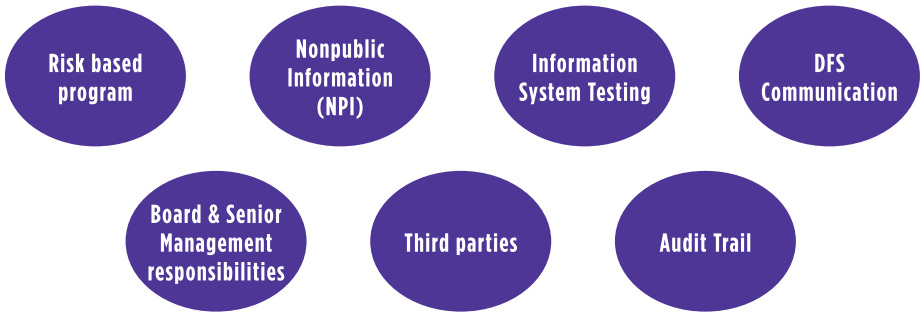
Supplementing the Graham Bliley Act requirements on data protection, the NYS regulation described the expectations of the capabilities dedicated to the protection of the NPI of the organization. The "intent to protect" will have to be complemented by a commitment on the results with the proper testing to prove it.

Furthermore, while the milestones for the regulation are spread across the coming years, the level of effort associated may vary greatly. The high-priority areas of initiatives are highlighted by Wavestone based on their complexity and their related amount of efforts.

Although some of these high-priority areas are not "due" in 2017, it is critical that banks initiate early enough the projects to complete them on time (see illustration bellow).

New York regulation is bringing the regulatory landscape one step further by embracing most of the cyber trends visible on the market. Most mature organizations won't have to revolutionize their approach to protect the organization and its data as long as a robust risk based framework was adopted. However the prioritization of the cyber-capabilities to be implemented could be impacted.

Therefore, financial institutions have to structure their cyber program to handle these new requirements as well as the upcoming regulations such as the Fed-OCC-FDIC Cybersecurity ANPR or the update on the cyber protection of the critical infrastructures. Regulation became indisputably a pillar of the cyber-roadmap that will balance the investments prioritization between compliance and cyber-resilience.



WAVESTONE GLOBAL CYBERSECURITY REGULATORY WATCH

In order to provide regulatory insights to our US clients impacted by global activities, our team conducts continuous surveillance of all major regulatory developments related to cyber risk management and data protection.

We monitor authorities and regulators from America, Europe, Asia and Africa to develop an informed view about worldwide regulatory trends. We also regularly interacts with the cyber risk and data protection communities in order to reinforce our understanding of the regulations and their impact on our clients' organizations. Our methodologies and frameworks are continuously updated to reflect regulatory changes.

Through this deep understanding, we are able to advise our clients on which actions need to be taken, and in what timeframe, both at the local and global levels.

With 100+ enacted rules & regulations from over 20 individual states, national regulators and authorities, the United States' regulatory environment is monitored with great scrutiny to shape our recommendations.

Meanwhile, global activities call of the consideration of additional global authorities and regulators as well.

WAVESTONE

www.wavestone.com

Wavestone is a consulting firm, created from the merger of Solucom and Kurt Salmon's European Business (excluding retails and consumer goods outside of France). The firm is counted amongst the lead players in European independent consulting.

Wavestone's mission is to enlighten and guide their clients in their most critical decisions, drawing on functional, sectoral and technological expertise.