NY Cyber Rules and Compliance

How to become compliant – and prove it.

KeepItSafe®

Recap

Effective date
March 1, 2017

Prove compliance
February 15, 2018

Entities covered
Any organization under the jurisdiction of New York, Department of Financial Services (NYDFS) and operating under or required to operate under a license, registration, charter, certificate, permit, accreditation, or similar authorization under the banking, insurance, or financial services law.

Exemptions criteria
- Fewer than 10 employees, including independent contractors, who are the firm's affiliates located in NY, or responsible for the business of the firm
- Less than $5m in gross revenue each of last three fiscal years from NY business operations
- Less than $10m in year-end total assets is calculated in accordance with generally accepted accounting principles, including assets of all affiliates

Table of Contents

Background

Due to the increase in data breaches and rise of ransomware attacks around the world, The New York State Department of Financial Services (DFS) has grown highly concerned about cybersecurity events affecting DFS-regulated financial services firms, as well as the risks posed to the industry at large.

Losses from breaches now exceed $400 million annually.

— Data Breach Investigations Report, Verizon, April 2015

On March 1, 2017, the New York DFS enacted new cybersecurity regulations (23 NYCRR 500) for all DFS-governed entities. Also known as "Cybersecurity Requirements for Financial Services Companies" ("NY Cyber Rules" for short), these regulations intend to establish regulatory minimum standards to foster the creation of effective cybersecurity programs in the financial sector.

These first-in-the-nation regulations represent the most stringent cybersecurity requirements in the United States, with an underlying goal of protecting customer information by securing the IT assets of regulated entities. These new rules affect virtually every aspect of IT security at financial firms and mandate that firms must assess their risk profile and design a program that mitigates the most serious cybersecurity risks. Commencing February 15, 2018, firms will be required annually to prepare and submit to the superintendent a Certification of Compliance with the NY DFS Cybersecurity Regulations.

"New York is the financial capital of the world, and it is critical that we do everything in our power to protect consumers and our financial system from the ever-increasing threat of cyber-attacks."

— Governor Andrew M. Cuomo

The frequency and severity of attacks, as well as the resulting breaches, pose a threat to the economy and to national security. Although organizations may resist regulation, there is value in protecting systems and data through standards and forced compliance; these guidelines give organizations a best-practices starting point to achieve reliable data protection.

Overview

Since the NY Cyber Rules affect nearly every aspect of IT security at financial firms, many affected institutions will still have challenges to implement an effective program within the required timelines. It's a lot for even mid-sized organizations to satisfy, even in spirit, much less practice.

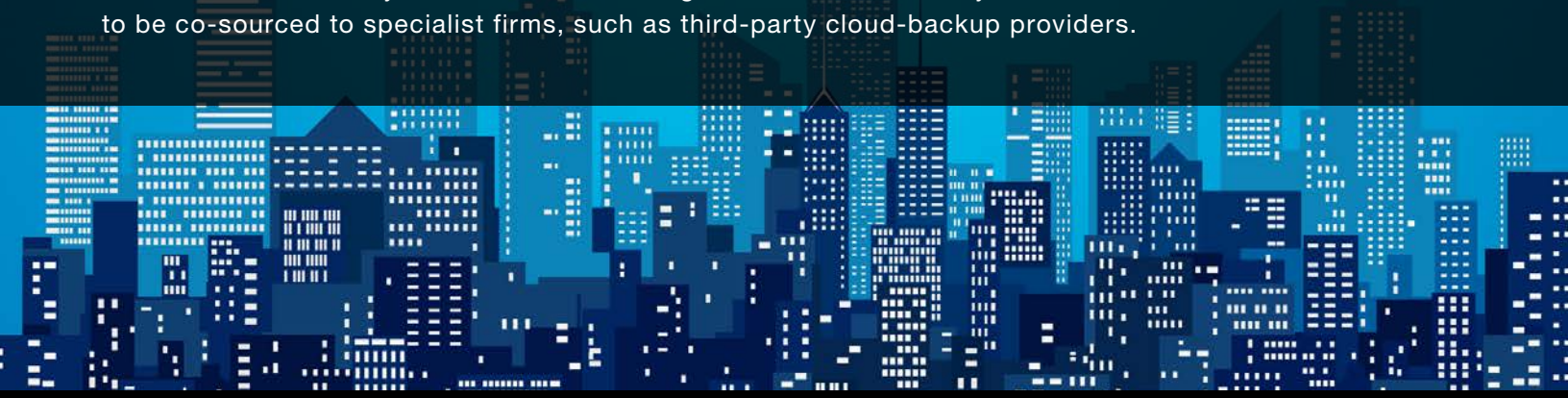
New York State enacted these regulations to set minimum requirements for protecting customer information in the financial-services sector, which includes banks and trust companies, insurance companies, mortgage lenders, investment companies, brokers, and other providers.

A purpose of this paper is to assist in providing background and guidance to firms so they may be on the safe side of NYDFS regulation compliance regarding best practices in cybersecurity, especially when it comes to third-party backup and cloud providers.

The core of the regulation requires that firms base IT security decisions on sound risk management practices. 23 NYCRR 500 covers the creation (or updating) of a firm's cybersecurity program. These NY Cyber Rules are NOT to be thought of as a recipe for complete security, but rather as guidelines for senior management. This guidance on establishing cybersecurity includes requirements that can be grouped into four major action principles:

1. Design a Cybersecurity Program
2. Implement a Cybersecurity Policy
3. Designate a Chief Information Security Officer
4. Select a Secure Third-Party Service Provider

Sub-sections of the rules also discuss steps financial firms should take regarding incident reporting policies, penetration testing, vulnerability assessments, access privileges, data protection and disposal, audit trails, and much more. Recognizing that many firms may not have the necessary skills in-house, the regulation allows for many of these functions to be co-sourced to specialist firms, such as third-party cloud-backup providers.

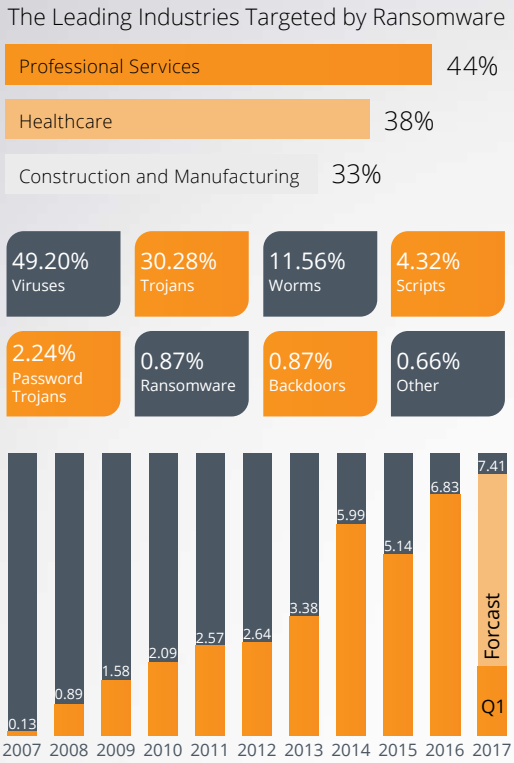


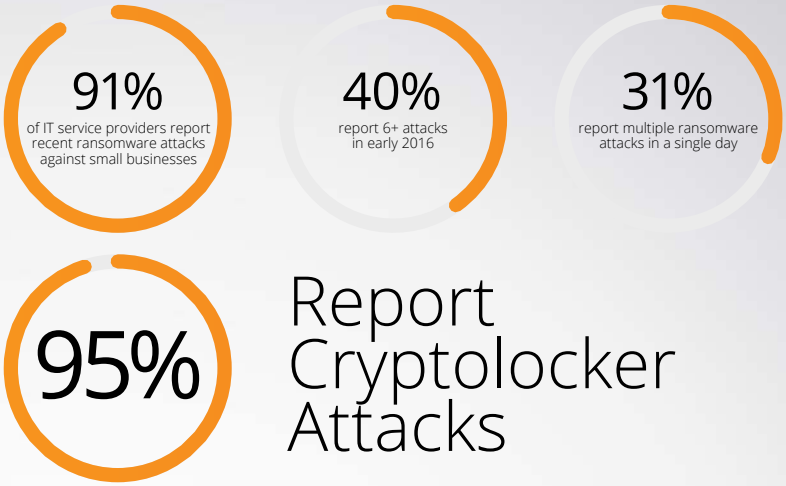
Minimum Requirements

To comply with the regulations, all organizations, regardless of size, revenue and assets, must have a cybersecurity program in place that consists of:

- Annual risk assessment of information systems
- Notice to the New York Department of Financial Services Cybersecurity Regulations superintendent when a cybersecurity event occurs
- A written cybersecurity policy
- Limited access privileges
- Limitations on data retention

Additional regulations may apply to your organization, depending on the number of employees (including independent contractors) that you have, your gross annual revenue and your year-end total assets. Check with the NYDFS for further information about the new regulations.





Less than 1 in 4 ransomware incidents are reported to the authorities

35% report ransomware attack on cloud-based applications, including Google Apps and Office 365.

70% of whom report Dropbox being the target.

Definitions

Definition of Information Systems

A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic information, as well as any specialized system

such as industrial/process control systems, telephone switching and private branch exchange systems, and environmental control systems.

Definition of Nonpublic Information: Nonpublic Information (NPI) is defined as all electronic information that is not publicly available information, and is:

- Business-related information
- Information concerning an individual, which, because of name, number, personal mark, or other identifier, can be used to identify such an individual when combined with SSN, driver's license, account number, security code, or biometric records.
- Any information or data, except age or gender, obtained from a health care provider that relates to an individual's past, present, or future physical or mental behavior for an individual or his/her family, including the provision of health care, and the payment for the provision of health care.

Definition of Third-Party Service Provider(s):

Third-Party Service Provider(s) (third party or third parties) means a person who;

(i) is not an affiliate of the Covered Entity.

(ii) provides services to the Covered Entity.

(iii) maintains, processes, or otherwise is permitted access to Nonpublic Information through the provision of services to the Covered Entity.

Design a Cybersecurity Program

Firms should establish and maintain an enterprise-wide cybersecurity program and policy that enable them to identify, measure, manage, and mitigate cyber risks. A key part of the establishment of a cybersecurity program includes performing a gap analysis to identify the most critical cyber risks in your company and to get an idea of where you will need to direct time and money to address those risks.

An initial penetration test will give you a baseline understanding of the degree to which your data is potentially vulnerable. These actions will give you direction about where to start developing your program.

- Identification of cyber risks
- Security policies and procedures
- Security emergency response procedures
- Comprehensive disaster recovery (DR) strategy
- Performance of an annual penetration test
- Quarterly vulnerability assessments

Program Purpose

Each firm shall maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of its Information System. The program shall be based on the entity's risk assessment and designed to perform the following core cybersecurity functions:

- Identify and assess internal and external cyber risks that may threaten the security or integrity of NPI stored on the entity's Information System
- Implement policies and procedures to protect the firm's information systems, and NPI stored on those systems, from unauthorized access, use, or other malicious acts
- Fulfill applicable regulatory reporting obligations
- Use defensive infrastructure
- Detect cybersecurity events
- Respond to identified or detected cybersecurity events to mitigate any negative effects
- Recover from cybersecurity events and restore normal operations and services

75%

75% of small business do not have a disaster recovery plan

Nationwide®

Implications

- Firms should evaluate their overall NPI definition to validate that they are in alignment with the NPI requirements.
- Firms should review their overall cybersecurity programs and create a repository to document their enterprise-level cybersecurity policy to determine that they cover the identified areas and maintain supporting program documentation

Compose an Incident Response Program

Firms should outline effective incident-response programs in place, as well as effective mechanisms to notify the DFS of material cyber events.

Incident Response

A firm's cybersecurity program 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 firm's information systems, or the continuing functionality of any aspect of the firm's business or operations. Such incident-response plan shall address:

- Internal processes for responding to a Cybersecurity Event
- Goals of the incident-response plan
- The definition of clear roles, responsibilities, and levels of decision-making authority
- External and internal communications and information sharing
- Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls
- Documentation and reporting regarding cybersecurity events and related incident-response activities
- Evaluation and revision of the incident-response plan following a Cybersecurity Event

DFS Notifications

Each firm 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:

- Cybersecurity events of which notice is required to be provided to any government body, self-regulatory agency, or other supervisory body; or
- Cybersecurity events that have a reasonable likelihood of harming any material part of the normal operations of the firm.

Implications

- Firms should reevaluate their incident-response plans to validate that they meet the new requirements; this includes determining the manner in which plans are enhanced, as required, after incidents have occurred — that is, that an effective feedback loop is in place.
- Firms should validate that their reporting protocols would provide for timely notification of matters to the DFS and, before that, provide for appropriate escalation within the company to senior management and, where necessary, the board of directors.

Implement a Cybersecurity Policy

The policy must cover several areas, including access controls, business continuity, third-party-provider management, and security incident response. Of all the areas that need to be covered by the policy, the ones that organizations tend to struggle with are data governance and classification. Knowing where data is, and what security level to assign to the data, is difficult yet important, and requires significant collaboration among information security (infosec) and IT operations teams.

Adopting an effective policy means that organizations must be capable of effectively monitoring systems and networks, and embedding security and quality assurance in the development lifecycle.

Policy Requirements

Each firm shall implement and maintain a written cybersecurity policy approved by a senior officer or board of directors that sets out procedures to protect its information systems and NPI stored on those systems. The cybersecurity policy shall be based on the entity's risk assessment and address the following:

- ✓ Information security
- ✓ Data governance and classification
- ✓ Asset inventory and device management
- ✓ Access controls and identity management
- ✓ Business continuity and disaster-recovery planning and resources
- ✓ Systems operations and availability concerns
- ✓ Systems and network security
- ✓ Systems and network monitoring
- ✓ Systems and application development and quality assurance
- ✓ Physical security and environmental controls
- ✓ Customer data privacy
- ✓ Vendor and third-party service provider management
- ✓ Risk assessment
- ✓ Incident response

Implications

- Firms should benchmark their standards, policies, and procedures against industry practices.
- Firms should dramatically expand the categories of data to encrypt and control, including:
  - Encrypt all “nonpublic information held or transmitted” in the firm
  - Restrict access privileges not only to systems but to the data itself
  - Implement an audit trail system to reconstruct transactions and log access privileges
  - Provide for the retention and “timely destruction” of non-public information

$209 Million

“Cyber-criminals collected $209 million in the first three months of 2016 by extorting businesses”

CNN

Risk Assessment, Testing, and Compliance

The NYDFS focus on risk assessment is unique because widely different business models are included under the same umbrella. Investment banking and electronic trading are as different from retail banking and credit-card processing as apples are to oranges. Firms should formally evaluate their cyber risks and the effectiveness of the related controls. Firms' systems and applications should be assessed routinely. When multi-dimensional risk assessments can be run across all systems in the environment, ascertaining the level of cyber-security risk to daily business operations (and simplifying compliance reporting within the 72 hours specified by the NYDFS cybersecurity regulation) moves from wishful thinking into the realm of possibility.

Risk Assessment

Firms must conduct periodic risk assessments of their information systems sufficient to allow for revision controls to respond to technological developments, evolving threats, risks of its business operations, and NPI collected or stored. The risk assessment shall be documented and follow written policies and processes, including:

- Criteria for assessing the confidentiality, integrity, security, and availability of the firm's information systems and NPI, including the adequacy of existing controls in the context of identified risks
- Criteria for evaluating and categorizing cybersecurity risk or threats
- Requirements for describing how risks will be mitigated or accepted and how the cybersecurity program will address the risks

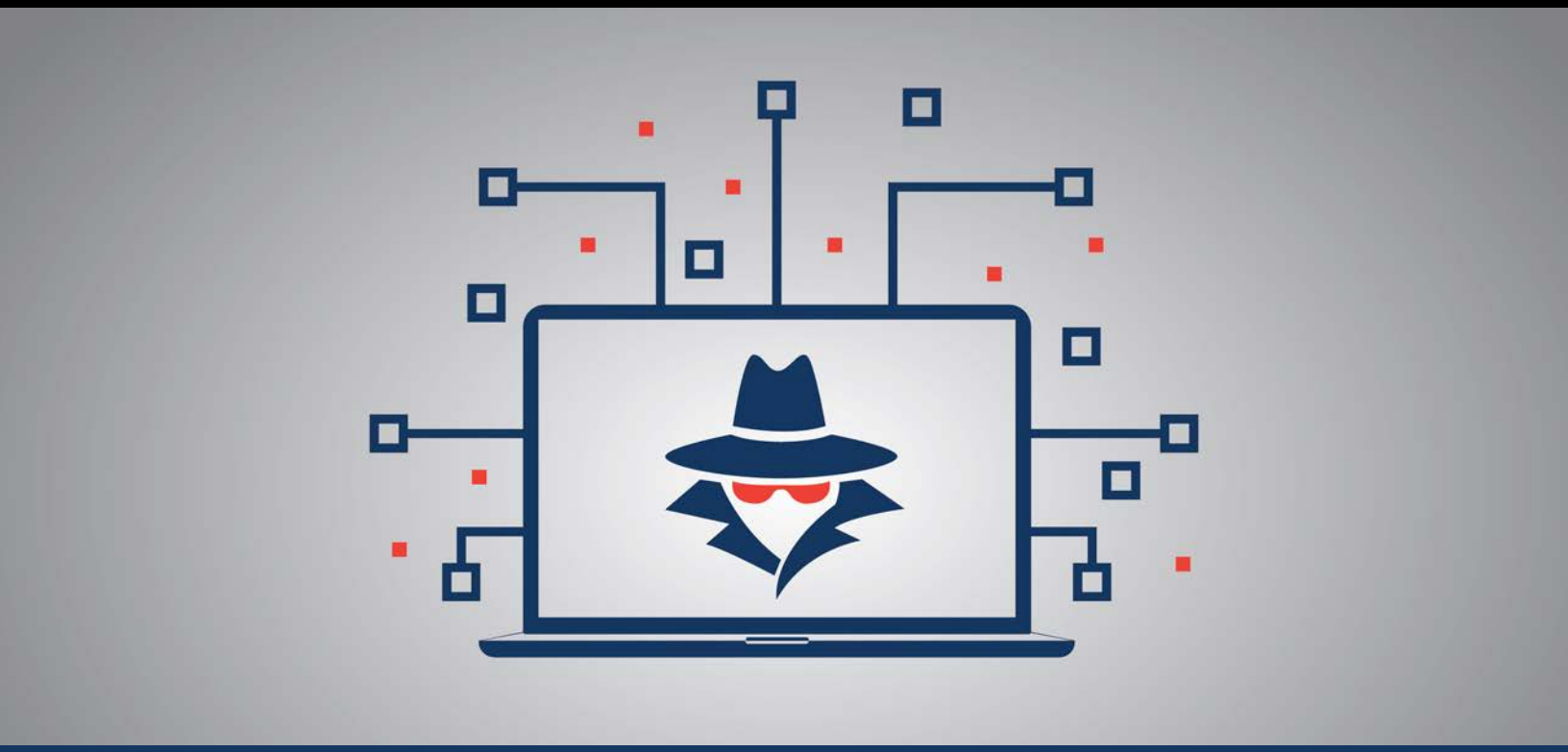
Penetration Testing and Monitoring

The cybersecurity program for the entity shall include monitoring and testing, developed in accordance with the entity's risk assessment. The monitoring and testing shall include continuous monitoring, or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring for ongoing detection vulnerabilities, firms shall conduct:

- Annual penetration testing of the firm's Information System based on relevant risks identified in accordance with the risk assessment
- Biannual vulnerability assessments, including systematic scans or reviews designed to identify publicly known cybersecurity vulnerabilities
- Implementation of risk-based policies, procedures, and controls designed to monitor the activity of authorized users, and detect unauthorized access or use, or tampering with NPI

Annual Compliance Representation

By February 15 of each year, entities shall submit to the superintendent a written statement covering the prior calendar year, certifying that they are in compliance with the requirements set forth. This documentation and supporting data must be available for inspection by the NYDFS superintendent, and help for a period of five years.



Implications

- Firms should review their cyber risk assessment approach to validate that it effectively evaluates the evolving cyber risks facing them, as well as the effectiveness of their cyber risk controls to address identified risks, to ensure they promote prompt and thorough remedial action, when required.
- Firms should evaluate the frequency and effectiveness of their penetration testing and vulnerability assessment strategy and techniques.

Data breach exposed the personal data of 143 million consumers

EQUIFAX

Designate a Chief Information Security Officer

The shortage of good security talent in the market does not make this an easy requirement to meet. The right Chief Information Security Officer (CISO) will have technical, management, strategic, and compliance audit skills, and must report directly to the board of directors. For most companies, getting the proper person in this role will mean hiring from the outside rather than promoting a security manager from within. If your organization does not feel confident that they have the right skills already on the bench, a better option may be hiring a CISO as a service from a third-party service provider that has a track record of providing similar services.

Firms should appoint a strong cybersecurity leader and verify they have the right people, resources, and firm-wide cybersecurity training.

Chief Information Security Officer

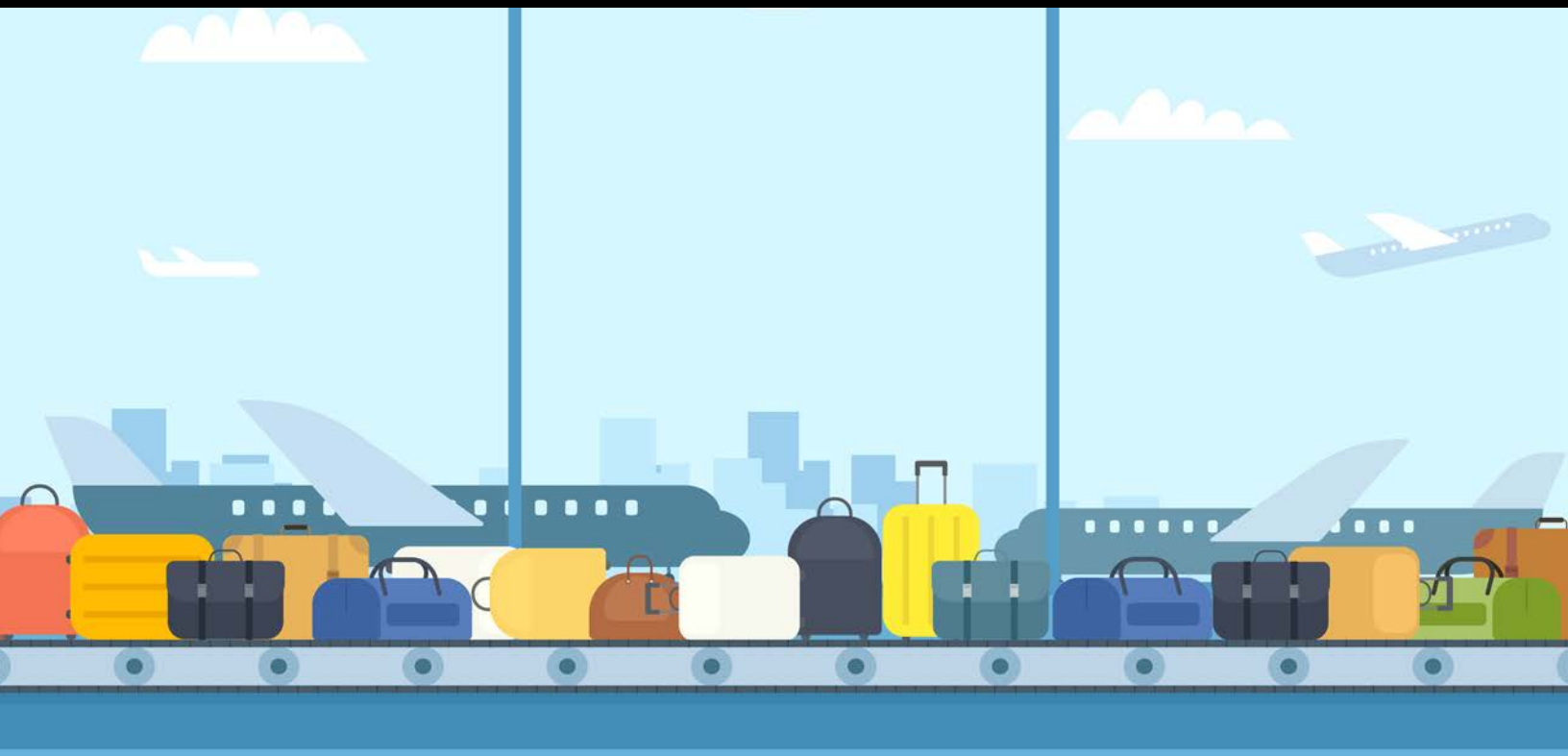
- Each firm shall designate a qualified individual to serve as the CISO, who is responsible for implementing, overseeing, and enforcing the firm's cybersecurity program and policy.
- At least annually, the CISO shall report to the board of directors or governing body in writing on the firm's cybersecurity program and material cybersecurity risks. The CISO shall consider to the extent applicable:
    - The confidentiality of NPI and the integrity and security of the firm's information systems
    - The firm's cybersecurity policies and procedures
    - The firm's material cyber risks
    - The overall effectiveness of the firm's cybersecurity program
    - Material cybersecurity events that affected the firm during the time period addressed by the report

Personnel and Resources

Each firm should utilize qualified cybersecurity personnel, an Affiliate or Third Party Service Provider sufficient to manage its cybersecurity risks, and to perform or oversee the performance of the core cybersecurity functions outlined in its cybersecurity program.

Training

- Each firm shall:
    - Provide cybersecurity personnel with cybersecurity update and training sessions sufficient to address relevant cybersecurity risks
    - Verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures
    - Provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the firm in its risk assessment



Implications

- Firms should assess their cybersecurity organizational structure and determine the appropriate placement and reporting lines of the CISO. Special attention should be paid to the independence of the CISO. Firms may need to revise roles and responsibilities across the first and second lines of defense.
- Firms should reassess their resource and personnel needs in light of the new requirements, and should review and potentially enhance periodic and ongoing cybersecurity training provided to personnel.

$82 Million

A Southwest Airlines computer system 1-hour outage could cost the company $82,000,000

Southwest

Access, Application Security And Encryption

Firms should effectively manage access and application security, and should encrypt NPI or develop plans to be able to do so.

Access Privileges and Authentication

- Access privileges: A firm's cybersecurity program based on its risk assessment shall limit user access privileges to information systems that provide user access to NPI, and shall periodically review such access privileges.
- Multifactor authentication (MFA): Based on its risk assessment, each firm shall use effective controls, which may include MFA or risk-based authentication to protect against unauthorized access to NPI or information systems. MFA shall be used for any individual accessing the firm's internal networks from an external network, unless the firm's CISO has approved in writing the use of reasonably equivalent or more secure access controls.

Application Security

- A firm's cybersecurity program shall include written procedures, guidelines, and standards designed to ensure the use of secure development practices for in-house-developed applications used by the firm, and procedures for evaluating, assessing, or testing the security of externally developed applications used within the firm's technology environment.
- All procedures, guidelines, and standards shall be periodically reviewed, assessed, and updated, as needed, by the CISO (or qualified designee) of the firm.

Encryption of NPI

As part of a firm's cybersecurity program, and based on its risk assessment, it shall implement controls that include encryption to protect NPI held or transmitted by the firm both in transit over external networks and at rest.

- If the firm determines that encryption of NPI in transit over an external network is not feasible, the firm may instead secure NPI using effective alternative compensating controls reviewed and approved by the firm's CISO.
- If the firm determines that encryption of NPI at rest is not feasible, the firm may instead secure NPI using effective alternative compensating controls reviewed and approved by the firm's CISO.
- To the extent that the entity is using compensating controls for the encryption of NPI, the feasibility of the encryption, and the effectiveness of the compensating controls, shall be reviewed by the CISO at least annually.

Implications

- Firms should review their access privileges and authentication approach — and those related to application security — to validate they meet the new standards and are in line with industry practices.
- Firms should review their approach to NPI encryption, and to the extent they will be relying on compensating controls in lieu of encryption they should work with their CISO to develop a transition plan to phase out these controls.
- Firms should consider their secure development practices as well as testing of externally developed applications for security measures.

Select a Secure Third-Party Service Provider

Along with appointment of a CISO, this is probably one of the areas that organizations will find most challenging. Your third-party service providers, including cloud backup and Disaster Recovery-as-a-Service (DRaaS) ,must also meet requirements around minimum cybersecurity practices. Make sure you have the requirements written into your contracts to avoid misunderstandings and disagreements later. It is recommended to create an internal checklist for choosing a vendor to help you ensure that you've set the right compliance expectations.

Firms should implement rigorous third-party cybersecurity risk management policies and procedures across the full data protection life cycle from creation, to off-site online storage with their third parties. Off-site cloud backup ensures that your data is always secure, accessible and easily recoverable in the event of an emergent data event.

Best practices and many regulations require data to be backed up and stored offsite. Onsite backups tend not to pass an audit. KeepItSafe® Online Backups and KeepItSafe DR can automatically store your data quickly and securely, while exceed NYDFS compliance standards.

Third parties

Each firm shall implement written policies and procedures designed to ensure the security of information systems and NPI that are accessible to or held by third parties. Such policies and procedures shall be based on the risk assessment of the firm, and shall address to the extent applicable:

- Identification and risk assessment of third parties to service providers
- Minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the firm.
- Due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers.
- Periodic assessment of Third Party Service Providers based on the risk potential and the continued adequacy of their cybersecurity practices.

Such policies and procedures shall include guidelines for due diligence and/or contractual protections related to Third Party Service Providers, including applicable guidelines:

- The Third Party Service Provider's policies and procedures for access controls, including use of MFA to limit access of systems and NPI
- The Third Party Service Provider's policies and procedures for the use of encryption to protect NPI in transit and at rest
- An incident notice to the firm in the case of a Cybersecurity Event directly affecting the firm's information systems or NPI being held
- Representations and warranties addressing the Third Party Service Provider's cybersecurity policies and procedures that relate to the security of the firm's information systems or NPI

2,315,931

2,315,931 global users encountered ransomware between Apirl 2015 and March 2016

KASPERSKY lab

Implications

- Firms should review their third-party/vendor risk-management standards, policies, and procedures to verify they meet the new requirements; this should include evaluating the manner and frequency with which they conduct off-site and on-site cybersecurity assessments of third parties.
- Firms should review their procurement/contracting process — and standard terms for third parties — to validate that all of the necessary new provisions are covered.
- Firms should determine how to implement these standards for existing as well as new third parties.

Compliance Pedigree

For more than a decade, KeepItSafe has been a world leader in compliant cloud backup, disaster recovery, endpoint protection, and SaaS application availability — serving more than 20,000 corporate customers across four continents, and protecting more than 50 petabytes of mission-critical data every year.

We offer global data availability and fully managed and monitored services with comprehensive 24/7 support. In fact, we are among the only global recovery providers awarded ISO 27001 certification for information security management.

If you have only limited familiarity with the major data-privacy regulations, you might assume they apply only to a few specific types of high-profile businesses. Regulatory federal compliance is commonplace with KeepItSafe from HIPAA, which governs the healthcare industry, to Sarbanes-Oxley, which applies to publicly traded companies (and all of their wholly owned subsidiaries), SEC Exchange Act (Rule 17A-4), and the Gramm-Leach-Bliley Act (GLBA), which deals with data-privacy banking rules.

But this New York regulation defines “data protection” extremely broadly, to include any organization that engages in financial activities as part of its normal business operations within the state of New York. This means that many other types of companies, which wouldn’t identify themselves as financial institutions, are subject to the rules of 23 NYCRR 500 — businesses such as real estate brokerages, insurance agencies, investment advisors, and collection agencies. Even retailers might fall under these regulations if they offer their own credit cards to customers.

This combination of broad regulatory reach and the KeepItSafe compliance pedigree can alleviate the regulation confusion and facilitate secure data protection. KeepItSafe meets the required NY Cyber Rules regulations including:

- FIPS 140-2 certification
- Worm media
- Delete lock
- Index search
- Audit trails
- 256-bit encryption
- Letter of compliance
- Designated third party

The KeepItSafe team is available to keep you on the compliance path by providing the data security needed — along with the required regulation proof with a Third -Party Service Provider Letter of Compliance.

77%

77% increase in DRaaS related inquires in 2016

Gartner®

KeepItSafe's Cloud Collection

The Cloud Collection portfolio includes a global reach to cloud data availability, and implores a holistic approach to provide seamless and continuous data protection—no matter where your data resides.

KeepItSafe Online Backup:

The industry's most secure, scalable, and easy-to-manage cloud backup and on-demand data recovery service — offering Backup-as-a-Service (BaaS) with fully managed and monitored 24/7 support.

KeepItSafe Disaster Recovery:

An all-in-one disaster recovery and online backup solution — offering fully managed and monitored Disaster Recovery-as-a-Service (DRaaS) that replicates and protects data across multiple off-site secure servers, and provides failover in the event of any emergent event.

KeepItSafe Mobile Backup:

Powerful endpoint backup, file sharing, collaboration, and data-loss prevention in one unified solution. KeepItSafe Mobile provides IT managers with the control they need to protect their enterprise against unforeseen data catastrophe.

KeepItSafe Cloud2Cloud:

Take control of your cloud application data with our SaaS backup solution. KeepItSafe Cloud2Cloud lets you bridge the gap between where your SaaS provider leaves off and real data protection begins.

Conclusion

The New York State regulations are likely the opening salvo in what will certainly be a growing framework of regulations and standards surrounding data and application cybersecurity. The federal government in the U.S. may follow in the footsteps of New York and adopt its own framework, while other countries will continue to introduce regulatory frameworks — like the General Data Protection Regulation (GDPR) in Europe.

All of this represents new challenges for firms in the financial services field, yet affect companies worldwide that have business dealings in New York State. The common denominator is that an implementation of best-practice standards, designing a comprehensive data-protection and disaster-recovery strategy, and leveraging a third-party for secure off-site cloud backup data protection can streamline compliance and simplify adherence. More importantly, they provide a foundation for a stronger cybersecurity program and a better-protected enterprise.

The good news: these regulations will reduce the risk of external attacks for your firm, and can reduce the risk of data breaches or data loss from insider threats, negligence, ransomware, hardware failure, and natural disasters.

Even better, KeepItSafe's Cloud Collection of global cloud data-availability solutions is your simple and seamless go-to data-protection answer to help your team meet enhanced data-security compliance regulations, scale to an off-site secure cloud, and be ready to face of future cybersecurity.

Free Webinar

Join our **free webinar** to learn from subject matter experts from KeepItSafe, PricewaterhouseCoopers, and Dragon Slayer Consulting to discuss what you need to know and do to be in compliance of New York's Cybersecurity Regulation (23 NYCRR Part 500) also known as the NY Cyber Rules, and the consequences of NOT being in compliance.

Contact Us

To learn more about our industry-leading solutions for cloud backup, disaster recovery, endpoint protection, and SaaS availability, contact us any time to schedule your free Network Evaluation and Data Protection Assessment, as well as to begin a free trial of our solution.

Website
www.KeepItSafe.com

Email
sales@keepitsafe.com

Phone
888.965.9988