Ensuring NYDFS Compliance with EPP, EDR, and Cybersecurity Services

Meeting New York State Financial Security Compliance Regulations

CYLANCE

"*The financial services industry is a significant target of cybersecurity threats…given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted.*" **— The New York Department of Financial Services**

Introduction

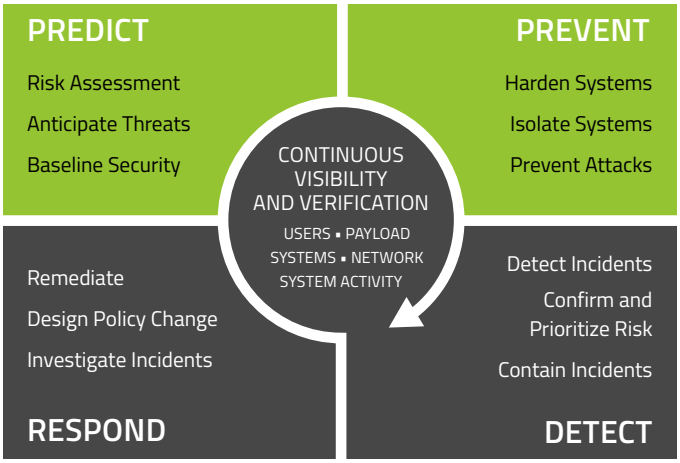
Given the advent of new and ever-changing compliance regulations, including recent mandates from the New York Department of Financial Services (NYDFS), security professionals need to have a full understanding of the updated regulations and how they impact endpoint protection platforms (EPP), endpoint detection and response (EDR) solutions, and the need for augmented security services and consulting.

On March 1, 2017, the NYDFS Cybersecurity Requirements went into effect as defined under 23 NYCRR Part 500. The new rule applies to nearly 1,900 banking and other financial institutions with assets of more than $2.9 trillion, and all insurance companies that do business in New York. Over 1,700 insurance companies with assets exceeding $4.2 trillion are also included under this umbrella. The rules affect licensed lenders, state-chartered banks, trust companies, service contract providers, private bankers, mortgage companies, insurance firms doing business in New York, non-U.S. banks licensed to operate in New York, financial firms with offices in New York, and many other organizations. NYDFS mandates cast a wide net — far beyond just financial firms operating in New York.

While many of the existing compliance rules prescribe specific actions or requirements, the NYDFS guidelines focus on a cybersecurity program risk assessment to determine the efficacy of a firm's best practices and policies to mitigate cybersecurity risks. Section 500.02 outlines requirements for an established and effective cybersecurity program to identify risks and detect and respond to cyber events. Section 500.03 specifies that written policies and procedures, including those pertaining to EPP and EDR, must be in place to protect information. Section 500.05 requires continuous penetration testing and vulnerability assessments, and 500.06 discusses the need for audit trails. Section 500.09 relates to a Covered Entity's overall risk posture and requires assessments to determine the ability to detect and respond to cyberthreats and mitigate risks and damage.

One of the more important Sections is 500.16, which discusses the need for an incident response plan. Under part (b) item (5), the NYDFS requires Covered Entities to identify requirements to remediate weaknesses in information systems and associated controls. Given the advent of new reports from Gartner and other analyst firms, which expose the weaknesses of legacy EPP and EDR solutions, ignorance is no longer an adequate excuse. When assessing whether a Covered Entity is compliant, the NYDFS will point to these reports and question why a Chief Information Security Officer (CISO) is continuing to use inadequate solutions.

This white paper is designed for Information Technology (IT) and Information Security (IS) professionals and technology-focused executives, and reviews the NYDFS mandates and their impact on Covered Entities as related to EPP, EDR, and security consulting services,



Source: Gartner (September 2017)

The Security Landscape

Nearly all IT and security professionals are familiar with Gartner's Magic Quadrant, which visually depicts vendor ratings on a four-quadrant graph. These professionals often review cybersecurity reports and updates from Gartner, as they are considered one of the industry's most accurate thought leaders. Gartner recently released a cybersecurity analyst report titled *Redefining Endpoint Protection for 2017 and 2018.* This groundbreaking report states that malware, ransomware, zero-day attacks, and other malicious attack tools, tactics, and techniques are evolving faster than traditional endpoint protection platforms. As such, organizations must now ensure that employed EPPs and EDRs have also evolved and can adequately detect and defend against constantly changing and expanding attacks.

Gartner recommends adopting their Adaptive Security Architecture framework to assess a firm's ability to detect, investigate, and respond to security threats. Their new report discusses this architecture and shows how EPP and EDR solutions are converging. Additionally, why next generation platforms should include more advanced technologies such as artificial intelligence and machine learning. The Gartner *Redefining Endpoint Protection for 2017 and 2018* analyst report, combined with *The Next-Generation Anti-Malware Testing for Dummies* book, can help Covered Entities ensure they are fully compliant with the looming NYDFS mandates.

Data Security Statutes

Financial, insurance, banking, and related firms typically need to comply with regulatory mandates related to the Federal Trade Commission Act, FINRA, PCI-DSS, Gramm-Leach-Bliley, and others. While these controls have been in place for some time, regulators recently determined that most are not adequate enough to deal with escalating security threats. As such, the NYDFS created a new, more encompassing set of regulations that the agency introduced in 2017.

What Is the NYDFS 23 NYCRR Part 500?

According to a recent report from IBM X Force, the average financial services firm experiences 65% more cyberattacks than organizations in other industries. In 2016, the number of malicious attacks against financial services firms escalated to 1,684 as compared to 1,310 the prior year. In response, New York became the first U.S. State to propose cybersecurity rules and regulations for financial organizations. To ensure compliance, NYDFS granted a six-month transitionary period to allow firms time to comply. By February 15, 2018, Covered Entities must be able to demonstrate full compliance by submitting annual Certifications of Compliance.

Definition of Information Systems:

Within the mandates, NYDFS refers to an Information System that represents "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 controls systems, telephone switching, private branch exchange systems, and environmental control systems."

The NYDFS uses this definition to include sensitive systems and data that must be safeguarded against cybercrimes and endpoint security threats.

Definition of Nonpublic Information (NPI)

The NYDFS also refers to Nonpublic Information (NPI), which means "all electronic information that is not Publicly Available Information" and contains business related data concerning an individual that can be used to identify him or her by name, number, personal mark, or other identifier, in combination with social security number, driver's license number or non-driver identification card number, account number, credit or debit card number, any security code, access code, or password that would permit access to an individual's financial account, or biometric records.

The new rules will reduce the risk of data breaches caused by endpoint or insider threats, ignorance, or unintentional data leakage.

Definition of Third-Party Service Provider(s)

This refers to a person or entity that's not an affiliate of the Covered Entity, provides services to the Covered Entity, and maintains, processes, or otherwise is permitted access to NPI through its delivery of services to the Covered Entity. This might include a security services consultant or managed security services provider (MSSP). This is an important aspect, as many organizations not classified as a financial services firm may be affected and could still be considered a Covered Entity.

How Will the NYDFS Regulations Impact You?

NYDFS regulations require Covered Entities to comply with the following requirements by the dates indicated. Organizations affected by these guidelines must review and understand what's required and ensure compliance by the dates noted. You can find more information about this at 23 NYCRR Part 500.

August 28, 2017

- Establish a cybersecurity program
- Create and follow a set of cybersecurity policies
- Assign an internal CISO or utilize a third-party service provider
- Limit and periodically review user access privileges
- Hire internal or third-party qualified cybersecurity personnel
- Establish a written incident response plan

February 15, 2018

- Submit initial certification of compliance

March 1, 2018

- Establish periodic penetration testing and vulnerability assessments
- Conduct periodic risk assessment of information systems
- Use multi-factor authentication or risk-based authentication
- Provide regular cybersecurity awareness training
- Deliver an annual report by the CISO to the board of directors on the cybersecurity program and any risks

September 3, 2018

- Maintain records and audit trails
- Establish and follow guidelines for application security
- Limit data retention and establish proper procedures for safe data disposal
- Monitor and detect unauthorized access of sensitive information
- Encrypt and protect nonpublic data in motion and at rest

Liabilities

The consequences to Covered Entities that do not comply with the new NYDFS mandates can include fines, lawsuits, public exposure, loss of trust, and more. Potential real-world scenarios for non-compliance might include revocation of licenses and fines of up to $250,000. Under New York Consolidated Laws, Banking Law - BNK § 44, subsection (b), penalties for violations can be as high as $25,000 per day.

Beyond NYDFS fines, firms are subject to NY State fines, breach disclosure consequences, and potential lawsuits for violating Gen. Bus. Law Article 39-F, §899-AA), and NY City Admin. Code Title 20, Chapter 1, §20-117. Even prior to the implementation of the recent mandates, the NYDFS gained a reputation for heavy-handed enforcement. In 2016, the agency collected billions of dollars in fines and settlements from dozens of leading financial institutions for compliance

violations. New regulation guidelines under 23 NYCRR Part 500 will only increase the agency's reach and the severity of non-compliance.

NYDFS Best Practice Recommendations

To ensure full compliance, there are several best practices that Covered Entities should consider. Initially, IT and IS professionals should undertake a comprehensive security assessment to find any gaps and identify areas of weakness or non-compliance. Below are five primary areas of focus under the new NYDFS mandates that should be reviewed to ensure compliance:

Overall Program and Policy Framework

Covered Entities will need to establish and maintain an organization-wide cybersecurity program and policies that will enable them to identify, measure, manage, and mitigate risks. NYDFS modifications from the original proposal include:

- Documentation related to an organization's cybersecurity program must be available for inspection by the superintendent upon request
- A cybersecurity policy must be based upon an organization's risk assessment
- The asset inventory and device management program must be included in an organization's cybersecurity policy
- The cybersecurity policy must be approved by the CISO (or third-party provider) instead of by the board of directors

The best practices recommendations to comply with these changes include:

- Evaluate your firm's NPI definition to validate that you're aligned with the NYDFS rules
- Employ third-party security service experts to assess your cybersecurity programs and create and maintain a document repository of cybersecurity policies
- Benchmark your cybersecurity policies, standards, and procedures against industry best practices and determine how your firm compares to others

Risk Assessment, Testing, and Compliance

Covered Entities should formally evaluate cybersecurity risks and the effectiveness of their organizational controls. All related systems and applications should be assessed and evaluated on a continuous basis — not just by the dates noted. Of most importance is a review and assessment of current EPP and EDR solutions to ensure they are adequate. For example, the Gartner EPP report specifically states that "Malware and attack tools, tactics, and techniques are evolving faster than the protection capabilities delivered by traditional endpoint protection platforms."

NYDFS modifications from the original proposal include:

- The risk assessment process was changed from annually to periodic, and should include enough information to assess the design of your cybersecurity program as defined by the NYDFS mandates
- Monitoring and vulnerability/penetration testing requirements are now continuous and/or periodic based on your overall risk assessment
- The date to provide a written statement to the superintendent about your compliancy is now February 15 of each year and covers the certification for the prior year

The best practices recommendations to comply with these changes include:

- You'll need to review your cyber risk assessment approach to validate that it effectively covers evolving cybersecurity risks, including an evaluation of current EPP and EDR efficacy — the Gartner EPP report says that "Traditional EPPs are focused on preventing the initial infection, but miss the rest of the adaptive security architecture tasks, such as hardening, incident detection and incident response"
- You'll need to consider using third-party security services to determine the effectiveness of your controls to address identified risks, and your ability to promptly undertake the required actions
- You should evaluate the frequency and effectiveness of your breach and penetration testing, and vulnerability posture, strategies, and detection/remedial techniques — if your current EDR solution does not adequately detect and respond to current and future threats, a change may be advised

Personnel, Resources, and Training

You will need to employ a strong cybersecurity leader and verify they have the right people, resources, and organizational cybersecurity training. NYDFS modifications from the original proposal include:

- Your CISO can now be employed at your firm, or you can use third-party security services
- Your CISO's requirements for reporting to your board of directors should be annual and in writing, and should focus on material cybersecurity events instead of all events
- Your cybersecurity training requirements must be based on the risk scenarios identified as part of your risk assessment process — if you don't have robust training in place, consider working with a security services provider to do this

The best practices recommendations to comply with these changes include:

- Assessing your cybersecurity structure and determining appropriate reporting guidelines for your CISO
- Revising various roles and responsibilities, especially for your CISO, across your cybersecurity lines of defense
- Reassessing your IT and IS personnel and resource requirements, and matching them against the new NYDFS mandates, as well as ensuring periodic and effective training

Access, Application Security, and Encryption

You'll need to effectively manage EPP, EDR, and application security solutions to ensure you have properly and adequately protected NPI, or at least have an adequate plan in place to do so. NYDFS modifications from the original proposal include:

- Your CISO now needs to implement a periodic, rather than an annual, review of application security guidelines, standards, and procedures
- Encryption requirements are now based on what's feasible or not feasible for your firm by determining various compensating controls as reviewed and approved by your CISO
- Multi-factor authentication is now required and has been updated from covering only specific types of access to determining what your critical access paths and informational assets are based on your risk assessment, and protecting against unauthorized access to any NPI

The best practices recommendations to comply with these changes include:

- You'll want to review your NPI encryption and EPP/EDR protection capabilities and understand how they might rely on compensating controls instead of adequate encryption or endpoint protection — especially as related to mobile and cloud access
- Your CISO should establish a plan to move beyond compensating controls to employing compliant encryption and protection for all NPI
- You should review your security development practices and testing for your externally-developed security measures and applications
- You'll need to review your firm's access privileges and authentication approaches, and EPP and EDR capabilities, especially as related to application security, and validate that you're complying with the new mandates

Optimize Your Business

One of the more difficult aspects of ensuring compliance with the looming NYDFS mandates is doing so without causing user or IT disruption, especially when implementing EPP and EDR for mobile and cloud access. Three ways to do this include:

- Using EPP and EDR solutions that are simple and fast to deploy and integrate with a wide variety of other solutions — augment and replace rather than rip and replace
- EPP and EDR solutions should be easy to manage and scale, and include local agents and a lightweight enterprise architecture
- Any EPP and EDR solutions and security services employed should enable "silence" as related to user complaints and business roadblocks by eliminating daily scans and mitigating cumbersome IT and IS management tasks

Ensure Continuous Attack and Threat Prevention

The new NYDFS mandates require initial and periodic assessments to ensure adequate safeguards against malicious attacks that could expose NPI. Here are three considerations to ensure compliance that can easily pass any risk assessment:

- Predictive artificial intelligence and machine learning solutions provide future proof protection against new zero-day and advanced persistent threats
- Ensure any EPP or EDR solutions deployed offer a wide breadth of detection, response, and proactive prevention for any attack type (ransomware, malware, fileless attacks, etc.)
- Facilitate "silence" in your organization as related to NYDFS audit failures through EPP and EDR solutions that include device, script, and application control, memory protection, and security consulting services that ensure adequate assessments and policy adherence

Drive Predictability

Many of the NYDFS rules focus on driving predictability around a Covered Entity's cybersecurity posture, and adequately assessing and measuring any risks. To accomplish this, consider these three best practices:

- Reduce attack surfaces and allow for accurate and predictable budgets, timelines, and initiatives by employing the latest EPP and EDR solutions that are future proof
- Ensure your EPP and EDR solutions offer fast and simple integration with a wide variety of applications, and facilitate robust reporting and C-Level metrics
- Guarantee "silence" from board members, executives, and auditors by way of measurable, predictable, and scalable enterprise-class EPP and EDR solutions, along with proven security consulting services that identify and prioritize risks though penetration tests, assessments, and social engineering

Conclusions

To reduce security risks and ensure compliance with NYDFS and other regulatory mandates, EPP and EDR should be assessed for efficacy and compliance, and updated immediately where needed. Enterprise compliance should be adequate and efficient, and should not overly burden an organization or create roadblocks to business growth or IT and IS initiatives. Instead, any EPP, EDR solutions, or security consulting services should optimize the business, prevent successful attacks, and drive measurable predictability. Doing so requires proactive artificial intelligence endpoint protection, detection, and response solutions that ensure painless, reliable, and affordable compliance, coupled with consulting services that can help prevent assessment or audit failures.

About Cylance®

Cylance is revolutionizing cybersecurity with products and services that proactively prevent, rather than reactively detect, the execution of advanced persistent threats and malware. Our technology is deployed across more than ten million endpoints and protects hundreds of enterprise clients worldwide, including Fortune 100 organizations and government institutions.

For more information, visit us at www.cylance.com.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

20180208-0169