SOLUTION GUIDE

9 NYDFS Cybersecurity Requirements That You Can Tackle with Rapid7

RAPID7

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).

The purpose of the regulation is to require organizations to establish and maintain a "risk-based, holistic, and robust security program" that is designed to protect consumers' private data.

The requirements are widespread and range from more general guidelines, such as maintaining a cybersecurity program, to specifics like maintaining an audit trail. Luckily, you don't need to enlist a different security vendor to help you with each requirement. Rapid7 products and services can help you with almost all of them, and we have consultants standing by to help you put a plan in place.

Who's Affected?

Broadly, the requirements cover any organization operating under or required to "operate under DFS licensure, registration, or charter, or which are otherwise DFS-regulated, as well as, by extension, unregulated third-party service providers to regulated entities."

This includes:

- state-chartered banks
- licensed lenders
- private bankers
- service contract providers
- trust companies
- mortgage companies
- foreign banks licensed to operate in New York
- insurance companies doing business in New York

It does EXEMPT companies with less than 10 employees, less than $5 million in gross annual revenue for three years, or less than $10 million in year-end total assets.

IMPORTANT DATES

March 1, 2017
New requirements became effective

August 28, 2017
New requirements to be implemented

February 15, 2018
Required annual Certifications of Compliance begin

What You Need to Do

(And How Rapid7 Can Help)

Firstly, and most significantly, this DFS regulation requires covered entities to file an annual certification of compliance with the regulation. These Certifications of Compliance will commence February 15, 2018.

According to the regulation, in order for organizations to reach the goals of the compliance, organizations must implement the following:

1. **Cybersecurity Program (Section 500.02)**
   Establish a cybersecurity program based on periodic risk assessments and designed to identify and assess risks; protect information systems and nonpublic information; detect, respond to, and recover from cyber events; and fulfill all reporting obligations.
   - Rapid7 Consulting offers a variety of **Program Development** services designed to help you build, maintain, and measure the core cybersecurity functions of your program. Program development offerings are available for vulnerability management, risk management, incident response, security policies, and security program metrics.
   - Using **InsightIDR** and our ability to correlate LDAP, Active Directory, and DHCP not only helps identify and keep track of all assets in your environment, but can also identify unauthorized access and other malicious behavior through our user-behavior analytics, deception technology, and agents.
   - Rapid7 **Nexpose** allows you to conduct frequent vulnerability assessments and identify the assets that pose the most risk, by using exploitability, malware exposure, and vulnerability age to show you which assets would be easiest to breach in an attack (and how to fix them). Live dashboards allow you to quickly assess how your overall program is doing and where risk is being reduced.

2. **Cybersecurity Policies (Section 500.03)**
   Create and maintain written policies and procedures for the protection of information systems and nonpublic information and based on the company's risk assessment.
   - The security policy **Program Development** offering evaluates the comprehensiveness of your current set of cybersecurity policies and provides you with new or updated policy language that will set the standard for the implementation of security controls within your organization.

3. **Chief Information Security Officer (Section 500.04)**
   Designate a CISO to oversee and implement the cybersecurity program. The CISO may be employed by the regulated entity, an affiliate, or a third party service provider.
      - Rapid7's **Virtual CISO** service provides your organization with trusted security advisors to help guide security efforts, strategy and execution plans. The Virtual CISO works as an integral part of your security team and provides extensive experience in information security program assessment, development, and management.

4. **Penetration Testing and Vulnerability Management (Section 500.05)**
   The cybersecurity program must include continuous monitoring or annual penetration testing and bi-annual vulnerability assessments.
      - **Penetration Testing Services** from Rapid7 gives you a real-world look at how attackers could exploit your vulnerabilities – and guidance on how to stop them. Our team not only performs +1,000 penetration tests yearly, but is also dedicated to ongoing security research, making them as close to real-world hackers as you can get.
      - **Metasploit Pro** makes it easy for novices and experts alike to conduct end-to-end penetration tests; by doing penetration testing in house, you save money in the long run and can integrate regular penetration testing into your other security processes.
      - **Nexpose**, Rapid7's leading vulnerability management solution, allows you to continuously assess, prioritize, and remediate vulnerabilities. It uses a combination of agents, Adaptive Security, and connection to our SONAR research project to provide continuous monitoring of assets for new vulnerabilities.

5. **Audit Trail (Section 500.06)**
   Maintain systems designed to recover material financial transactions following an event and audit trails to detect and respond to Cybersecurity Events.
      - Rapid7's SIEM solution, **InsightIDR** processes all events against over 65 user behavior analytics and other techniques to detect Cybersecurity Events. Raw logs and endpoint data are ingested and enriched so they can be searched after any cybersecurity event. All activity is searchable for 90 days by default, but this is configurable, and archives can be marked for indefinite holding in cold storage, per the request of the client.
      - **InsightIDR** can flag systems as restricted assets, so that the solution will alert you on any change in behavior. This includes suspicious authentications, users with unexpected privilege escalations, and even approved users remotely accessing the asset from a new source asset. Specific users can be added to a watchlist. This will lower the threshold of the user behavior analytics on any alert that is generated.
6. **Application Security (Section 500.08)**
   Implement secure development practices and procedures for evaluating and testing the security of applications.
      - Our application security solution, **AppSpider**, crawls, interprets, and tests today's modern and complex apps, providing you with interactive and actionable vulnerability reports.

7. **Risk Assessments (Section 500.09)**
Conduct bi-annual risk assessments that consider threats, particular risks to the entity, and an examination of existing controls in the context of identified risk.
    - Rapid7's **Cyber Security Maturity Assessment** evaluates the effectiveness of your cybersecurity controls and provides you with a prioritized and risk-based security roadmap, as well as the detailed recommendations that allow you to move your security program forward with confidence.
    - **Metasploit Pro** can be used to conduct various forms of risk assessments throughout the year, from standard network penetration tests to social engineering and phishing campaigns. It can also be used to test that the rest of your security controls and programs are working properly and blocking/detecting the attacks they should.

8. **Cybersecurity Personnel and Intelligence (Section 500.10)**
Utilize qualified cybersecurity personnel or an "Affiliate or a Third-Party Service Provider" sufficient to manage the organization's risks and to perform or oversee the performance of the core cybersecurity functions.
    - Rapid7 **Managed Detection & Response** (MDR) becomes your SOC, staffed by some of the industry's most regarded security analysts and a threat intelligence operation. Rapid7 MDR is powered by our InsightIDR solution that combines the power of user behavior analytics, endpoint detection and response (EDR), and log analysis to unify security data in order to detect, investigate, and remediate incidents.

9. **Incident Response Plan (Section 500.16)**
Establish a written incident response plan for responding to and recovering from cybersecurity events.
    - The incident response **Program Development** offering evaluates your environment to rate your response capability and provides relevant, business-based recommendations to help you design and meet your IR program goals.
    - Rapid7 **Managed Detection & Response** (MDR) is your SOC, monitoring your environment, and ready to pivot to incident response at the first sign of a breach.
    - Rapid7 Consulting provides **Incident Response Services** to help in the event of a breach. Our team is ready to collaborate closely with your in-house team to detect threats, document findings, and recommend the right remediation activities to help ensure attackers are out and can't find their way back in.

Not quite sure where to start? We can help with that too. Contact us today to speak with a consultant about how Rapid7 can get you on the fast path to NYDFS compliance.

www.rapid7.com/contact