NYDFS 500
Simplifying the Second Amendment

Webinar broadcasted June 13, 2024

W/TH secure

Agenda

- Introductions
- NYDFS 500: A summary
- The key changes
- What hasn’t changed
- Our analysis of the key changes
- Q&A

Introductions

John Jarrold

- Security & Risk Management Consultant

Richard Suls

- Security & Risk Management Consultant

Miguel Gutierrez

- Security & Risk Management Consultant

A quick summary of the amendment

What’s changed? And what hasn’t?

500.1 Definitions

Changes

New Definitions:

- **Class A company** - covered entities with over 2,000 employees -or- $1B in gross annual revenue are subject to additional requirements
- **Cybersecurity incident** - an event which impacts the entity, has reasonable likelihood causing material harm, or results in deployment of ransomware. This was likely added to differentiate cyber events from cyber incidents
- **Independent audit** - an internal or external party free to make decisions without influence/interference. This definition aligns with the new requirement §500.02(c) to conduct independent audits of its cybersecurity program
- **Privileged account** - this definition aligns with the new requirements to limit provisioning/use of privileged access, and for class A companies to implement a privileged access management solution
- **Senior governing body** - the board of directors or most senior leadership of the covered entities. This definition aligns with the new requirements in §500.04(d) for senior level oversight of the cybersecurity program

Changes:

- **CISO** - no real change- just added what was originally documented in Section 500.4 Chief Information Security Officer to the definition section
- **Person** - added the qualifier "non-governmental"
- **MFA** - removed "text message on a mobile phone" from possession factors
- **Covered entity** - added the clause "regardless of whether the covered entity is also regulated by other government agencies."
- **Risk assessment** - added more specificity and aligned the definition to NIST
- **Third-party service provider** - added clarifying clause "is not a governmental entity"

Analysis

- New definitions and changes mainly reflect the updates to the regulation
- **Risk assessment definition is important as it prescribes criteria and approach for conducting assessments**

500.2 Cybersecurity program

Changes

- Class A companies must conduct **<u>independent audits</u>** of its cybersecurity program

Analysis

- **Auditor may be Internal or External**
- Independent - must be free to make objective and unbiased decisions without pressure or interference
- Frequency not prescribed but should be justified by the Risk Assessment
- Recommendations to demonstrate effectiveness:
    - Document Audit Procedures/Methodology which aligns with the Risk Assessment
    - **Ensure auditors have sufficient expertise in cybersecurity**

500.3 Cybersecurity policy

Changes

- Updates to original policy requirements:
  - Data governance, classification **and retention**
  - Asset inventory, device management **and end of life management**
  - Access controls, including **remote access** and identity management
  - Incident response **and notification**

- New policy requirements:
  - Security awareness and training
  - Vulnerability management

Analysis

- Data retention was an existing requirement under §500.13(b) but now must be codified in policy
- End of life management policy previously required, but specific requirements are not defined in §500.13 Asset Management except for a requirement to track support expiration dates in the asset inventory
  - **Managing legacy EOL technical debt can be a challenge due to dependencies, refresh cost, security and other factors**
- Remote access has no specific requirements except MFA, but should be limited to using the approved solution potentially other provisions for remote work security
- Incident notification policy should cover new requirements in §500.17(a)(1) and §500.17(c) discussed below
- Security awareness and training - policy now required, but cybersecurity awareness training was an existing requirement
- Vulnerability management policy requirement aligns with more prescriptive requirements in §500.5 Vulnerability Management.
  - **Ensure the VM policy is clear on the meaning of timely remediation of vulnerabilities**
- Password policy is required by §500.07(b) but not mentioned in this section

500.4 Cybersecurity governance

Changes

- Annual report to the board must include plans for remediating material inadequacies
- BoD Responsibilities
  1. Oversee cybersecurity risk management
  2. Possess sufficient cybersecurity knowledge
  3. Ensure cybersecurity program implementation and maintenance
  4. Confirm sufficient resources allocated to cybersecurity

Analysis

- Plans for remediating cybersecurity issues are likely included in most board reporting packages already
- BoD requirements are new to the NYDFS 500 amendment, but in many institutions the board will already have these responsibilities
  - **Ensure BoD awareness and understanding of their responsibilities, and provide support**
  - **Consider how to evidence how this requirements is being met e.g. meeting minutes and other communications**

500.5 Vulnerability management

Changes

- More specificity for penetration testing:
    1. from both inside and outside the information systems' boundaries
    2. by a qualified internal or external party
- New requirements for vulnerability scans:
    1. manual reviews of systems not covered by automated scans
    2. promptly after system changes
- Monitoring process to promptly inform of new security vulnerabilities
- Remediate vulnerabilities timely

Analysis

- Scope of pentesting may need to be expanded to meet the inside and outside requirement
- Hopefully pentests are already being performed by qualified personnel :-)
- Manual vulnerability reviews can be complex, cumbersome, ineffective, or infeasible
    - **Assess requirements for manual reviews and begin developing procedures**
- Re-scanning systems after material changes is likely already a practice – just ensure it is done consistently and can be evidenced
- Ensure monitoring for security advisories includes all systems (i.e. not just Windows and Linux)
- **Timely vulnerability remediation can be a significant challenge due to volume, complexity and coordination**

500.6 Audit trail

No Changes

500.7 Access privileges and management

Changes

Section has become much more prescriptive. New requirements include:

- Limit access to NPI
- Limit provisioning and use of **privileged accounts**
- Access recertification, existing requirement expanded to include: at a minimum annually and remove or disable accounts and access that are no longer necessary;
- Restrict remote access protocols
- Access termination for leavers
- Password policy
- Class A companies
    - **PAM solution**
    - **Automated blocking of weak passwords**

Analysis

- **Identify and manage entitlements that grant access to NPI** and:
    - Specify which job roles are approved for each entitlement
    - Use Role-Based Access Control tied to job roles where possible
    - Flag NPI entitlements in access requests to make it apparent to approvers
    - Require mindfulness in recertifying NPI access
- **Identify and plan for systems which will require custom solutions for blocking weak passwords**
- Identify privileged access, evaluate necessity and opportunities to reduce
- Limit use of privileged access through automation and immutable environments
- **Assess effectiveness of existing PAM solution or begin planning if not already in place**

500.8 Application security

No Changes

500.9 Risk assessment

Changes

- New requirement "at a minimum annually"
- Expanded definition §500.01(p):
  - **Old Definition**: *Risk assessment means the risk assessment that each Covered Entity is required to conduct under section 500.9 of this Part.*
  - **New Definition**: *Risk assessment means the process of identifying, estimating and prioritizing cybersecurity risks to organizational operations (including mission, functions, image and reputation), organizational assets, individuals, customers, consumers, other organizations and critical infrastructure resulting from the operation of an information system. Risk assessments incorporate threat and vulnerability analyses and consider mitigations provided by security controls planned or in place.*

Analysis

- Plan to conduct risk assessment annually if not doing so already
- **The more comprehensive definition aligns with NIST and was likely intended to address NYDFS concerns about quality, consistency and level of detail in covered entities' risk assessments**
- **Attention should be paid to the risk assessment as it foundational to many of the NYDFS 500 requirements. The clause "and based on the entity's risk assessment" appears throughout the regulation.**

500.10 Cybersecurity personnel and intelligence

No Changes

500.11 Third-party service provider security policy

Changes	Analysis
• **<u>Removed Limited Exception:</u>** *§500.11(c) - An agent, employee, representative or designee of a Covered Entity who is itself a Covered Entity need not develop its own Third-Party Information Security Policy pursuant to this section if the agent, employee, representative or designee follows the policy of the Covered Entity that is required to comply with this Part*	• Appears to be an edge case, but plan to document your own Third-Party Information Security Policy if your institution previously qualified for this exemption

500.12 Multi-factor authentication

Changes

- Multi-factor authentication shall be utilized for any individual accessing any information systems of a covered entity
- Entities that qualify for limited exemption under §500.19(a) only need to utilize MFA for:
  - Remote access
  - Third party applications
  - Privileged accounts.

Analysis

- Additional detail based on NYDFS response to inquires from WithSecure
  - **Federated SSO – MFA required for initial authentication but not at each access to federated systems**
  - **On Prem Workstations – MFA includes accessing a workstation regardless of the location of the computer (remote or on-premises)**
- Recommendations:
  - Assess gaps; develop strategy and roadmap
  - Engage and educate application owners
  - Use jump servers for legacy systems

500.13 Asset management and data retention requirements

Changes

- Produce and maintain a complete, accurate and documented asset inventory updated at a defined frequency and which tracks key information for each asset including:
  - Owner
  - Location
  - Classification or sensitivity
  - Support expiration date
  - RTO

Analysis

- This section is new. The original regulation required covered entities to have an Asset Inventory policy, but did not set specify requirements
- **Maintaining an asset inventory presents multiple challenges including managing automated discovery and manual updates, ensuring data quality, defining the scope of assets and their attributes, and integrating systems that should consume inventory data to perform functions such as vulnerability scanning**
- Recommendations:
  - Centralized, single source of truth (avoid multiple, overlapping departmental repositories)
  - Auto-discovery
  - Accountability for data quality and periodic data review and recertification by asset owners
  - Independent Data Quality review/audit
  - IT Asset Management and/or CMDB solutions

500.14 Monitoring and training

Changes

- Implement risk-based controls designed to protect against malicious code, including those that **monitor and filter web traffic and email** to block malicious content
- Class A Companies must also implement EDR and SIEM solution
- Cybersecurity awareness training must cover social engineering

Analysis

- **Heavy new requirements to implement tooling including web/email filters, EDR and SIEM**
- Entities may already have some or all of these solutions in place, but should **review effectiveness** of these controls as they will now be subject to NYDFS examination
- Cybersecurity awareness training likely already includes social engineering, but NYDFS made it an explicit requirement since most of the breaches suffered by covered entities since 2017 were the result of phishing

500.15 Encryption of nonpublic information

Changes

- Encryption must meet industry standards
- Removed option for effective alternative compensating controls for encryption in transit

Analysis

- **Assess if legacy systems support industry standard encryption**
- **Plan for compliance with NIST Post-Quantum Cryptography Standardization**
- Plan to implement encryption in transit if you were previously using ‘alternative compensating controls’

500.16 Incident response and business continuity management

Changes

- Added Root Cause Analysis and recovery from backups as requirements for Incident Response Plans
- New requirement to **develop and maintain BC/DR Plans**
- IR and BC/DR Plans must be distributed to employees responsible for implementation, and they must be provided with training
- IR and BC/DR plans and **ability to restore data from backups must be tested annually**
- New requirement to maintain backups protected from unauthorized alterations or destruction
- **Incident response and BC/DR plans must be tested annually** with all staff and management critical to the response

Analysis

- As with previous, entities may currently have these processes in place but should **assess effectiveness to prepare for NYDFS examinations**
- With BC/DR Planning now in scope, entities should ensure **centralized oversight/governance of the BC/DR program** is in place including documentation, test tracking and issue management
- Assess enterprise-wide backup procedures and data restore testing for adherence to new requirements, especially if performed in a distributed manner
- **Ensure incident response plans are tested through table tops and other exercises**

§500.17 Notices to superintendent

Changes

- Notice of cybersecurity incident
  - Scope expanded to include notification of cybersecurity incident at any affiliates or a third-party service provider
  - Notification must be submitted through form on NYDFS website
  - Continuing obligation to update the superintendent with material changes or new information
- Notice of compliance
  - Certification must be signed by the CEO
  - Certification must be based on sufficient data and documentation from various sources (officers, employees, outside vendors, etc.), and be retained for five years
  - New option to acknowledge non-compliance with identified section of the regulation. Must provide remediation timeline
- New requirements to report ransomware payments within 24 hours and provided written justification for having done so within 30 days

Analysis

- Reporting requirements have become **more intrusive**
- Requirement for **CEO to sign the certification** indicates NYDFS taking a harder line on accountability
- **New option to acknowledge non-compliance provides entities with more flexibility, but also carries the risk of missing committed timelines**
- With the new requirements for ransomware reporting, NYDFS likely looking to gain better visibility into how ransomware is impacting the industry and how to prevent it from further encouraging criminal activity

500.19 Exemptions

Changes

- Eased qualifications for exemption:
    - Employees: 10 --> 20
    - Revenue: $5M --> $7.5M
    - Assets: $10M --> $15M

Analysis

- For smaller entities, check if you now qualify for the revised exemption thresholds

500.20 Enforcement

Changes

- Raised the bar on what constitutes a violation: a single prohibited act or failure to meet an obligation:
  - Failing to secure or prevent unauthorized access to NPI due to noncompliance
  - Materially failing to comply with any section for a 24-hour period
- Identified factors for assessing penalties for violations

Analysis

- **Section §500.20(b) signals NYDFS may be more likely to issue penalties going forward**
- **Review the new section to understand NYDFS factors for assessing penalties. Themes include:**
  - **Cooperation and good faith versus recklessness**
  - **Prior violations and systemic issues**
  - **Violation severity and impact**
  - **Institution size and business volume**
  - **Penalties or sanctions imposed by other regulatory agencies**

Thank you for your interest