THE NY CYBERSECURITY REG HAS CHANGED. NOW WHAT?

Big I NY & Big I CT Education

Today's Format

- What changed?
- Who has to do it?
- What is the deadline?

Compliance Deadline Nov. 1, 2023

Limited Exemption Criteria Changed:

Was	***Is***
< 10 employees & independent contractors of entity and affiliates	< 20 employees & independent contractors of entity and affiliates
< $5 million gross annual revenue in each of last 3 fiscal years from all of entity's business operations and affiliates' New York operations	< $7.5 million gross annual revenue in each of last 3 fiscal years from all of entity's business operations and affiliates' New York operations
< $10 million in year-end total assets of entity & affiliates	< $15 million in year-end total assets of entity & affiliates

Compliance Deadline Nov. 1, 2023

Affiliate:

- Owns the entity (ex: bank)
- Owned by the entity (agency's subsidiary)
- Under common ownership with entity

Compliance Deadline Nov. 1, 2023

Completely Exempt From Regulation:

- Brokers who:
  - Do not use information systems or nonpublic information (NPI)
  - Have not been paid to act as a broker for at least a year
  - Are not otherwise covered

Compliance Deadline Nov. 1, 2023

Completely Exempt From Regulation:

- Insurance agents whose licenses are inactive

Compliance Deadline Nov. 1, 2023

Notices of Exemption MUST be submitted electronically on DFS website unless written permission given to submit another way

- Apply at least 30 days before filing due

Compliance Deadline Nov. 1, 2023

Enforcement

- Violation = committing 1 prohibited act – failing to meet a requirement
- Violations include:
  - Noncompliance results in failure to protect NPI
  - Material failure to comply in 24-hour period
- DFS will consider 16 factors when assessing penalty

Compliance Deadline Dec. 1, 2023

Cybersecurity Incident Reporting

Must report w/in 72 hours of determining incident has occurred

- At entity's business
- At affiliate's business
- At 3rd party service provider's business

Compliance Deadline Dec. 1, 2023

Cybersecurity Incident:

Cybersecurity event that:

- Impacts entity & requires alerting authorities
- Reasonably likely to materially impact material party of entity's normal operations
- Results in ransomware attack on material part of entity's info system

Compliance Deadline Dec. 1, 2023

Cybersecurity Incident Reporting

Entity must:

- Promptly provide any info DFS requests about the incident
- Update DFS with any material changes / new info previously unavailable

Compliance Deadline Dec. 1, 2023

Extortion Payments Reporting

If entity is involved in cyber event that results in entity making an extortion payment:

- Report payment to DFS w/in 24 hours
- Provide details to DFS w/in 30 days

Compliance Deadline Dec. 1, 2023

Certification of Compliance

- Written certification that entity materially complied with requirements in prior calendar year **OR**
- Written acknowledgement that entity did not materially comply with all requirements
- Must:
  - ID sections where non-compliant
  - Describe nature/extent of non-compliance
  - Confirm remediation is complete OR provide timeline for completion

Compliance Deadline Dec. 1, 2023

Certification of Compliance

Must be signed by:

- Highest-ranking executive & chief info security officer (CISO)

OR

- Highest-ranking executive & senior officer responsible for entity's cybersecurity program

Compliance Deadline Apr. 29, 2024

Cybersecurity Program

- Must be designed to protect info system & NPI
- Documentation & info must be provided to DFS on request
  - Includes cyber program maintained by affiliate if entity has adopted that program

Compliance Deadline Apr. 29, 2024

Cybersecurity Program

APPLIES TO "CLASS A" COMPANIES ONLY:

Must design & conduct independent audits of cyber program based on risk assessment

Class A Companies

> $1 billion revenue

OR

> 2,000 employees & > $20 million revenue

Compliance Deadline Apr. 29, 2024

Cybersecurity Policy

- Entity's senior officer or governing body must approve cybersecurity policy annually
- Cybersecurity procedures must be developed, documented & implemented based on policy

Compliance Deadline Apr. 29, 2024

Cybersecurity Policy

- Policy must now address all of these if they apply to the entity:

Data retention	IT asset/device end of life management
Systems security monitoring	Security awareness & training
Systems & application security	3rd party service provider management
Incident notification	Vulnerability management

Compliance Deadline Apr. 29, 2024

Vulnerability Management

DOES NOT APPLY TO LIMITED EXEMPT ENTITIES

- Cyber policy/procedures must include vulnerability management
- Designed to assess & maintain cyber program effectiveness

Compliance Deadline Apr. 29, 2024

Vulnerability Management

DOES NOT APPLY TO LIMITED EXEMPT ENTITIES

- Policies/procedures must ensure:
  - Annual internal & external penetration testing
  - Monitoring process for new security vulnerabilities
  - Prompt remediation of vulnerabilities
  - High priority for most serious risks

Compliance Deadline Apr. 29, 2024

Application Security

DOES NOT APPLY TO LIMITED EXEMPT ENTITIES

- Annual review/assessment/update of procedures, guidelines & standards for secure in-house application development

Compliance Deadline Apr. 29, 2024

Risk Assessment

- Risk assessment review & update must occur at earliest of:
  - Annually
  - When business or technology change causes material change to entity's cyber risk

Compliance Deadline Apr. 29, 2024

Cybersecurity Personnel & Intelligence

DOES NOT APPLY TO LIMITED EXEMPT ENTITIES

- The choice of an affiliate or 3rd party to assist in complying with reg is now subject to the Chief Information Security Officer (CISO) requirements as well as the 3rd party service provider requirements

Compliance Deadline Apr. 29, 2024

3rd Party Service Provider

- Provision exempting employees & others from requirements deleted – another section of the reg provides the same exemption

Compliance Deadline Apr. 29, 2024

Monitoring & Training

- Annual cybersecurity awareness training required for all personnel
  - Must include social engineering awareness training
  - Limited exempt entities have until Nov. 1, 2024
- Training must be updated to address risks identified in entity's annual risk assessment

Compliance Deadline Apr. 29, 2024

Exemptions

- Entity's wholly owned subsidiary exempt from regulation if covered by entity's cyber program
- Subsidiary must submit Notice of Exemption

Compliance Deadline Nov. 1, 2024

Cybersecurity Governance

DOES NOT APPLY TO LIMITED EXEMPT ENTITIES

- CISO's report to senior governing body must include plans for addressing material issues
- CISO must timely report to senior governing body or senior officer on material cyber issues
  - Significant cyber events
  - Significant changes to cyber program
  - Others

Compliance Deadline Nov. 1, 2024

Cybersecurity Governance

DOES NOT APPLY TO LIMITED EXEMPT ENTITIES

- Entity's senior governing body responsible for oversight of cyber risk management
  - Have sufficient understanding of cyber issues
  - Require management to implement cyber program
  - Receive & review cybersecurity reports
  - Confirm sufficient allocation of cybersecurity resources

Compliance Deadline Nov. 1, 2024

Encryption

DOES NOT APPLY TO LIMITED EXEMPT ENTITIES

- Entity must have written policy requiring encryption meeting industry standards
- May use alternative to encrypting stored data
  - CISO must review & approve in writing
  - CISO must review use of alternative at least annually

Compliance Deadline Nov. 1, 2024

Incident Response & Business Continuity Management

DOES NOT APPLY TO LIMITED EXEMPT ENTITIES

- Entity must have written plans with proactive measures to
  - Investigate & mitigate cyber events
  - Ensure operational resilience

Compliance Deadline Nov. 1, 2024

Incident Response/Business Continuity Management

- Plan must include:
  - Incident response plan for quick response to & recovery from cyber events
  - New items incident response plan must address
    - Recovery from backups
    - Post-event root cause analysis
    - Plan updates as necessary

Compliance Deadline Nov. 1, 2024

Incident Response/Business Continuity Management

- Plan must include:
  - Business continuity and disaster recovery plan (BCDR) designed to:
    - Ensure system availability
    - Protect employees, assets & NPI during cyber-related disruption

Compliance Deadline Nov. 1, 2024

Incident Response/Business Continuity Management

- BCDR plan must include:
  - ID essential assets, employees & competencies
  - ID supervisors responsible for implementing plan
  - Communications plan for contacting essential personnel
  - Procedures for prompt critical data recovery & info systems
  - Procedures for prompt resumption of operations

Compliance Deadline Nov. 1, 2024

Incident Response/Business Continuity Management

- BCDR plan must include:
  - Procedures for essential data backup and offsite storage
  - ID 3rd parties necessary to info systems operation

Compliance Deadline Nov. 1, 2024

Incident Response/Business Continuity Management

- Entity must:
  - Make plan copies accessible to employees
  - Train employees responsible for implementation
  - Annually test
    - Incident response & BCDR plans
    - Ability to restore systems & data from backups
  - Maintain & protect backups

Compliance Deadline Nov. 1, 2024

Exemptions

- Limited exempt entities must meet:
  - Multi-factor authentication (MFA) requirements
  - Cybersecurity awareness training for all personnel requirements

Compliance Deadline Nov. 1, 2024

MFA requirements Nov. 1, 2024 - 2025

- Limited exempt entities must use MFA for any individual accessing entity's internal networks from an external network
- MFA = authentication through at least 2 of these factors:
  - Knowledge factor (password)
  - Possession factor (token)
  - Inherence factor (biometric info such as face scan)

Compliance Deadline May 1, 2025

Vulnerability Management

DOES NOT APPLY TO LIMITED EXEMPT ENTITIES

- Vulnerability management policies & procedures must ensure entity conducts:
  - Automated scans of information systems
  - Manual review of systems not covered by scans
- Purpose is to find, analyze, & report vulnerabilities
- Scan frequency determined by risk assessment
- Prompt scan required after material system change

Compliance Deadline May 1, 2025

Access Privileges & Management

Entity must:

- Limit user access to systems containing NPI to only those user needs to perform job
- Limit number of privileged accounts
- Privileged Account = authorized user account / service account that permits user to perform security related functions off-limits to other users

Compliance Deadline May 1, 2025

Access Privileges & Management

Entity must:

- Limit privileged accounts' access functions to only those necessary to perform job
- Limit privileged accounts' use to only when performing functions requiring such access
- Annually review all user access privileges
- Remove or disable unnecessary accounts & access

Compliance Deadline May 1, 2025

Access Privileges & Management

Entity must:

- Disable or securely configure all protocols permitting remote control of devices
- Promptly terminate users' access privileges following departures
- Have written password policy meeting industry standards

Compliance Deadline May 1, 2025

Access Privileges & Management

APPLIES TO "CLASS A" COMPANIES ONLY

Entity must monitor privileged access activity & implement

- Privileged access management solution
- Automated method of blocking commonly used passwords

Compliance Deadline May 1, 2025

Monitoring and Training

DOES NOT APPLY TO LIMITED EXEMPT ENTITIES

Entity must implement risk-based controls designed to protect against malicious code

APPLIES TO "CLASS A" COMPANIES ONLY

Entity must implement

- Endpoint detection and response
- Centralized logging & security event alerting

Compliance Deadline Nov. 1, 2025

MFA

Limited exempt entities must use MFA for:

- Remote access to info systems
- Remote access to 3rd party apps that give access to NPI
- Privileged accounts (other than service accounts with no interactive login)

Compliance Deadline Nov. 1, 2025

MFA

- Non-exempt entities must use MFA for any user accessing any of entity's systems
- CISO may approve equivalent or more secure alternatives
  - Must review & approve annually

Compliance Deadline Nov. 1, 2025

Asset Management

- Entity must implement written policies & procedures for producing & maintaining info systems asset inventory

Compliance Deadline Nov. 1, 2025

Asset Management

- Policies & procedures must include:
  - Method to track asset information including:
    - Owner
    - Location
    - Classification or sensitivity
    - Support expiration date
    - Recovery time objectives
  - Required frequency for updating & validating inventory

Questions?

Resources

- www.biginy.org/cyber
- www.biginy.org/cyber-news
- https://www.dfs.ny.gov/industry_guidance/cybersecurity

Contact Info

Tim Dodge, AU, ARM, CPCU

(315) 432-4229

tdodge@biginy.org

THE NY CYBERSECURITY REG HAS CHANGED. NOW WHAT?

Big I NY & Big I CT Education