pillsbury

Are You Ready for November 1 & the New NYDFS Cybersecurity Requirements?

Mark Krotoski &
Brian Montgomery

OCTOBER 1, 2024

Presenters

Mark Krotoski

Partner | Cyber Disputes Leader
Litigation

Former National Coordinator for the Computer Hacking and Intellectual Property Program at DOJ Former Federal Cybercrime Prosecutor

Brian Montgomery

Senior Counsel | Consumer Finance Leader
Regulatory

Former NYDFS Deputy Superintendent

Agenda

- NYDFS Cybersecurity Regulation Overview
- November 1, 2024: New Requirements
  - Exemption standards
  - Governance requirements
  - Incident Response
  - Encryption
- Checklist & Investigation Best Practices
- Other Key Issues
- Legal Issues & Preparedness

pillsbury

NYDFS Cybersecurity Regulation Overview

Department of Financial Services Scope of Jurisdiction

The DFS monitors more than 3,000 financial institutions with assets totaling more than **$9.7 trillion**, including:

1,900+ insurance companies with more than $6.4T in assets

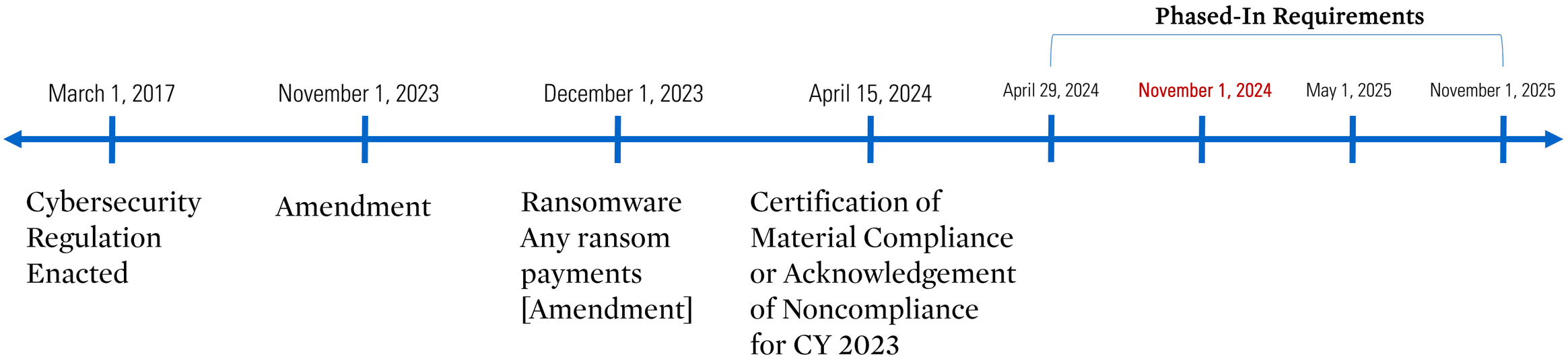
- Property/casualty insurance
- Life insurance
- Health insurance and managed care
- Pharmacy benefits managers

1,300+ banking and other financial institutions with more than $3.3T in assets

- State-chartered banks
- Foreign branches and agencies
- Virtual currency companies
- Credit unions

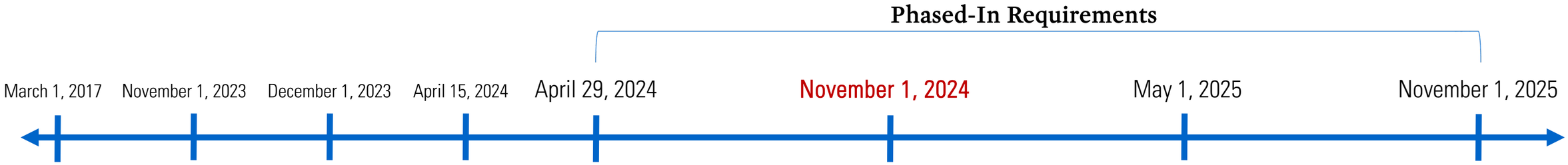
NYDFS Cybersecurity Regulation Overview

Covered Entities



NYDFS Cybersecurity Regulation Overview for Covered Entities

Covered Entities



- Risk assessments
- Update cybersecurity policies and procedures
- Annual penetration testing
- Annual awareness training

- Exemption standards
- Governance requirements
- Incident response
- Encryption

- Enhanced requirements regarding limiting user access privileges

- Automated scans of information systems, and a manual review of systems not covered by such scans
- Enhanced requirements on user access privileges

NYDFS Cybersecurity Regulation Overview for Covered Entities

Class A Requirements

April 29, 2024 – Adding Section 500.2(c)

- Design and conduct independent audits of their cybersecurity program

May 1, 2025 – Adding Section 500.14(b)

- Implement endpoint detection and response solution to monitor anomalous activity and centralized logging and security event alert solution
- CISO can approve reasonably equivalent or more secure compensating controls, but approval must be in writing

NYDFS Cybersecurity Regulation Overview for Covered Entities

Small Business

November 1, 2024

- Implement multifactor authentication (MFA) requirements in Section 500.12(a) if not already done.
- At least annual cybersecurity awareness training. [Section 500.14(a)(3)]

NYDFS Cybersecurity Regulation Overview for Covered Entities

Annual Submission of Certification of Material Compliance or Acknowledgement of Noncompliance [Section 500.17(b)(1)]

- By April 15th, for prior calendar year
- Signed by the highest-ranking executive and the CISO
- Submitted electronically
- Maintain records “for examination and inspection by” DFS “for a period of five years”

NYDFS Cybersecurity Regulation Examinations

Examination Process

- Safety and soundness and compliance examinations
- Cybersecurity-focused examinations

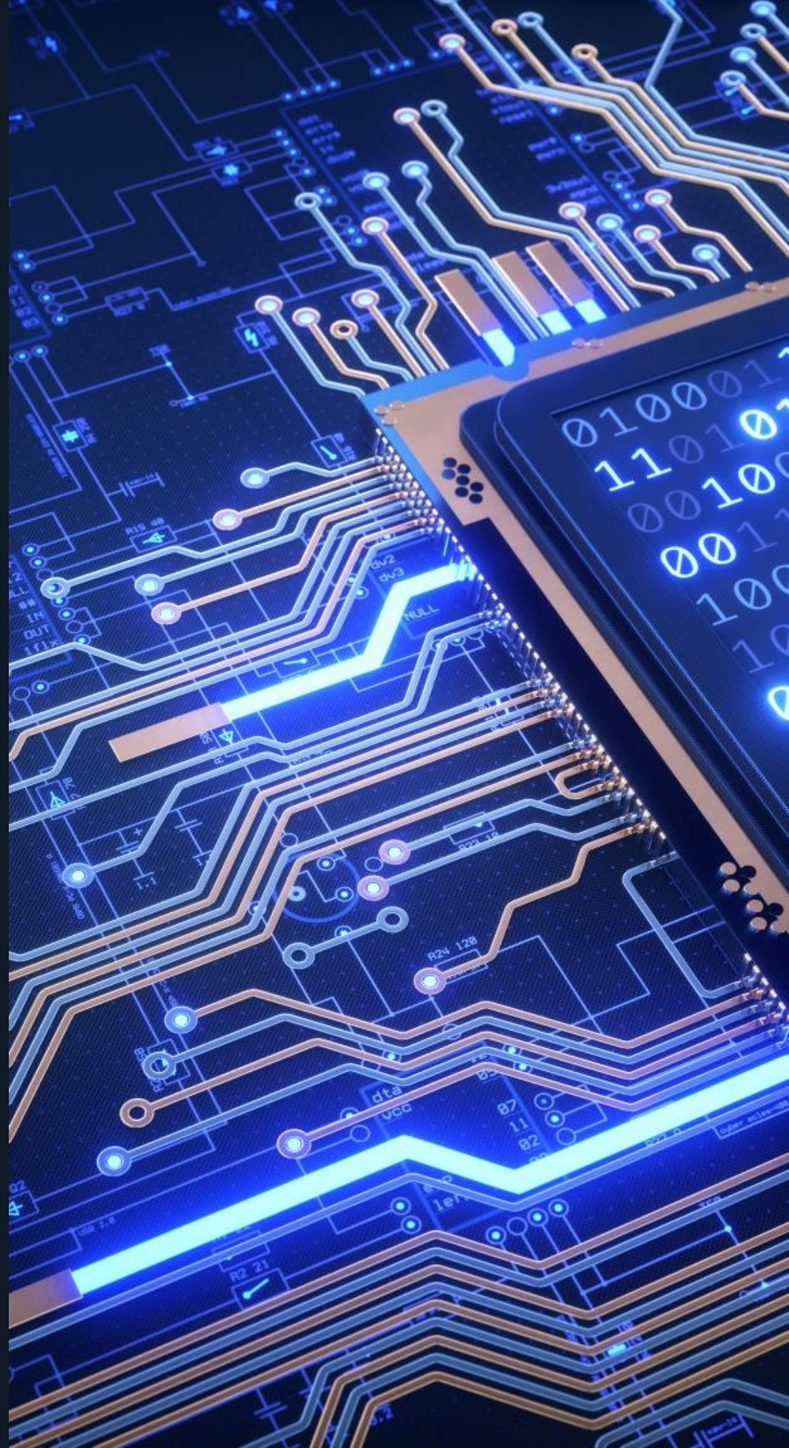
NYDFS Cybersecurity Regulation Overview

Cybersecurity program based on risk assessment [Sections 500.2]

- Covered entities must maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the covered entity's information systems and nonpublic information
- Must be based on the covered entity's risk assessment
- Factors
  - Risk may vary depending on type of business, size, information and other factors

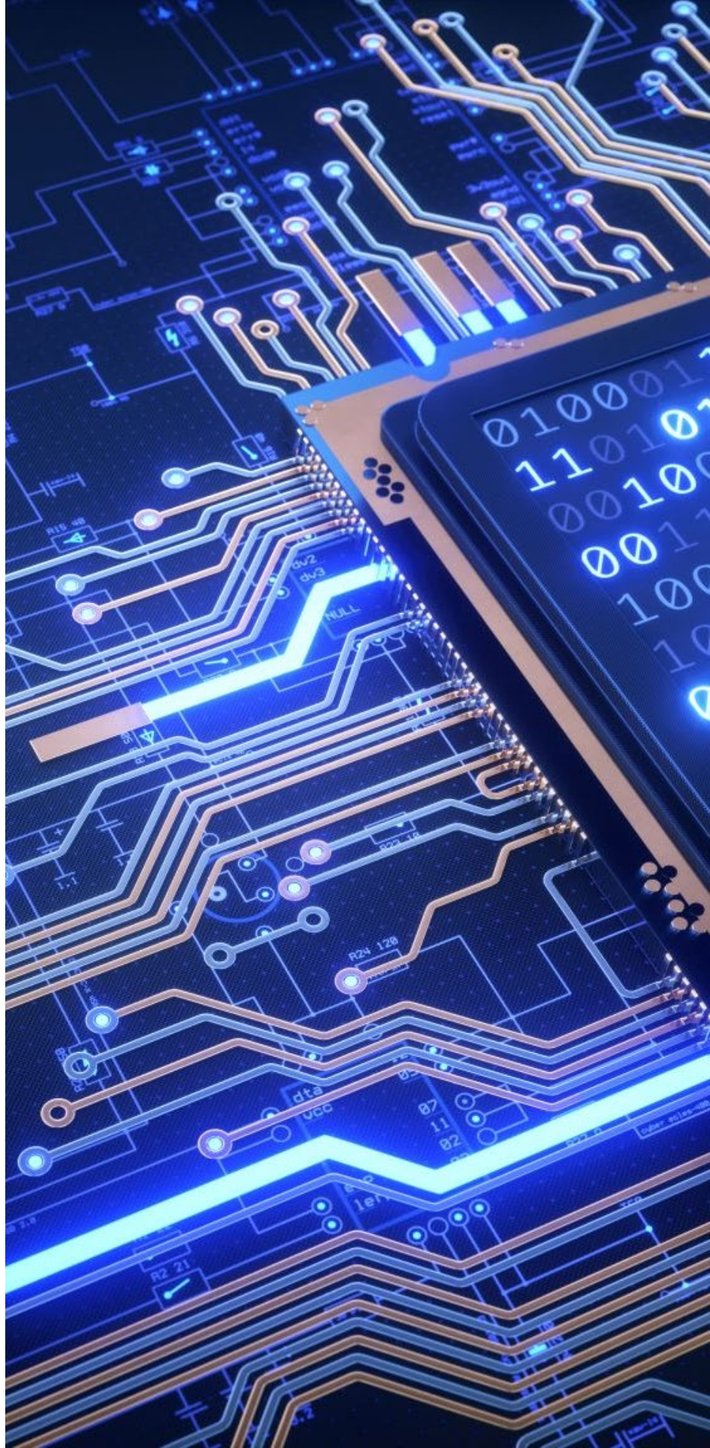
pillsbury

November 1, 2024: New Requirements



November 1, 2024: New Requirements

- Exemption standards
- Governance requirements
- Incident Response
- Encryption



Limited Exemption Standards [Section 500.19(a)]

November 1, 2024

Number of Employees

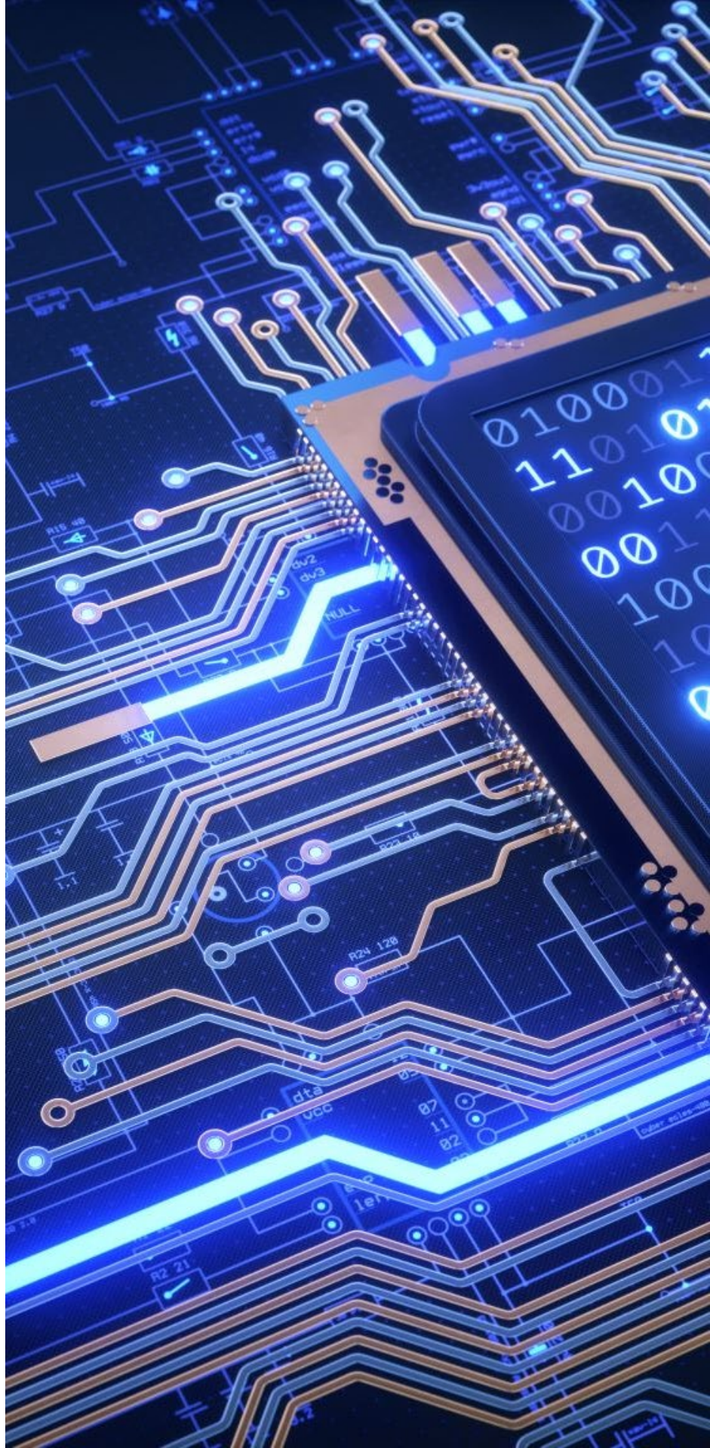
Change from fewer than 10 employees to fewer than 20 employees

Gross Annual Revenue

Change from less than $5,000,000 in gross annual revenue in each of the last 3 fiscal years from New York operations, to less than $7,500,000 in gross annual revenue in each of the last 3 three fiscal years from all operations

Year-End Total Assets

Change from less than less than $10,000,000 in year-end total assets, to less than $15,000,000 in year-end total assets

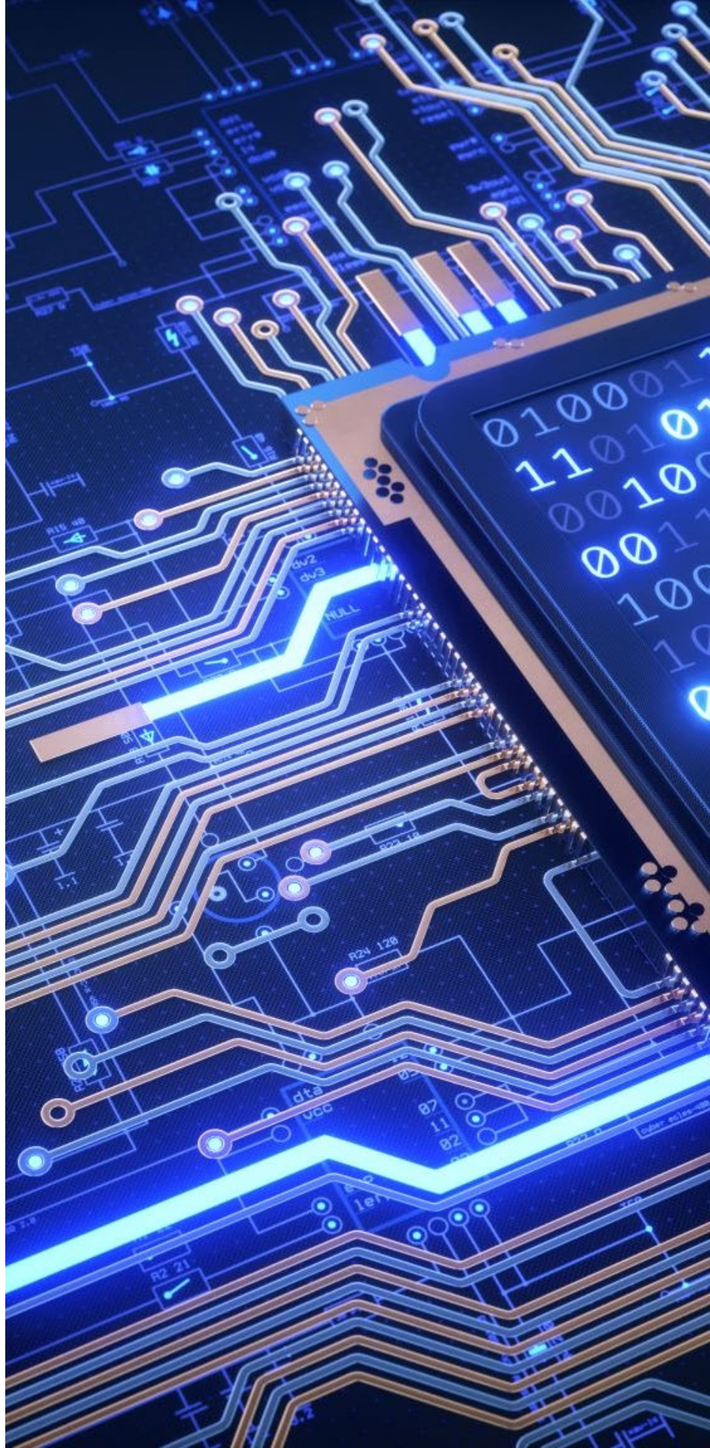


Governance Requirements [Section 500.4]

Existing Requirements for CISO's Annual Cybersecurity Program Report

CISO's annual written report to board (or senior governing body)

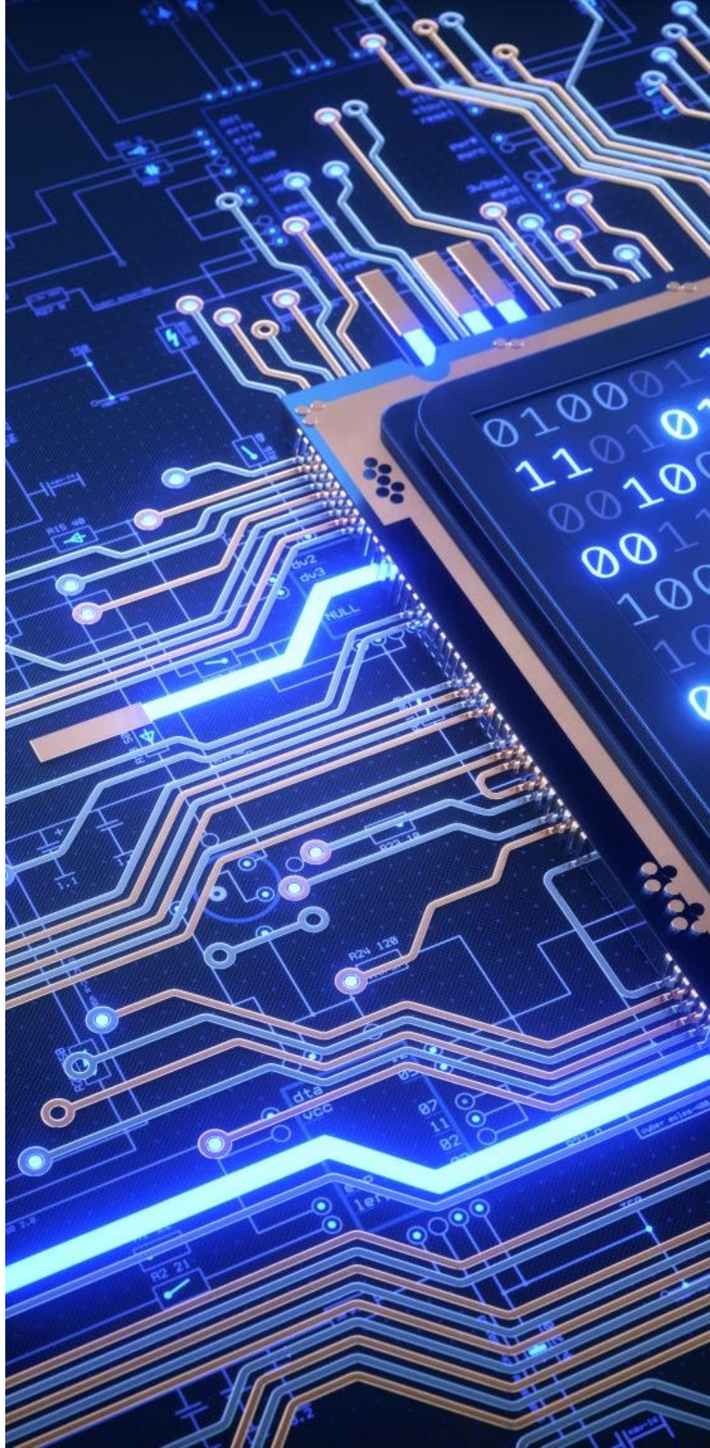
- The confidentiality of nonpublic information and the integrity and security of the information systems
- Cybersecurity policies and procedures
- Material cybersecurity risks
- Overall effectiveness of the cybersecurity program
- Material cybersecurity events during period addressed by the report



Governance Requirements [Section 500.4]

November 1, 2024

- CISO's written report to board (or senior governing body) updated to include plans for remediating material inadequacies
- CISO timely report to board or senior officers on material cybersecurity issues
  - Significant cybersecurity events
  - Significant changes to the cybersecurity program



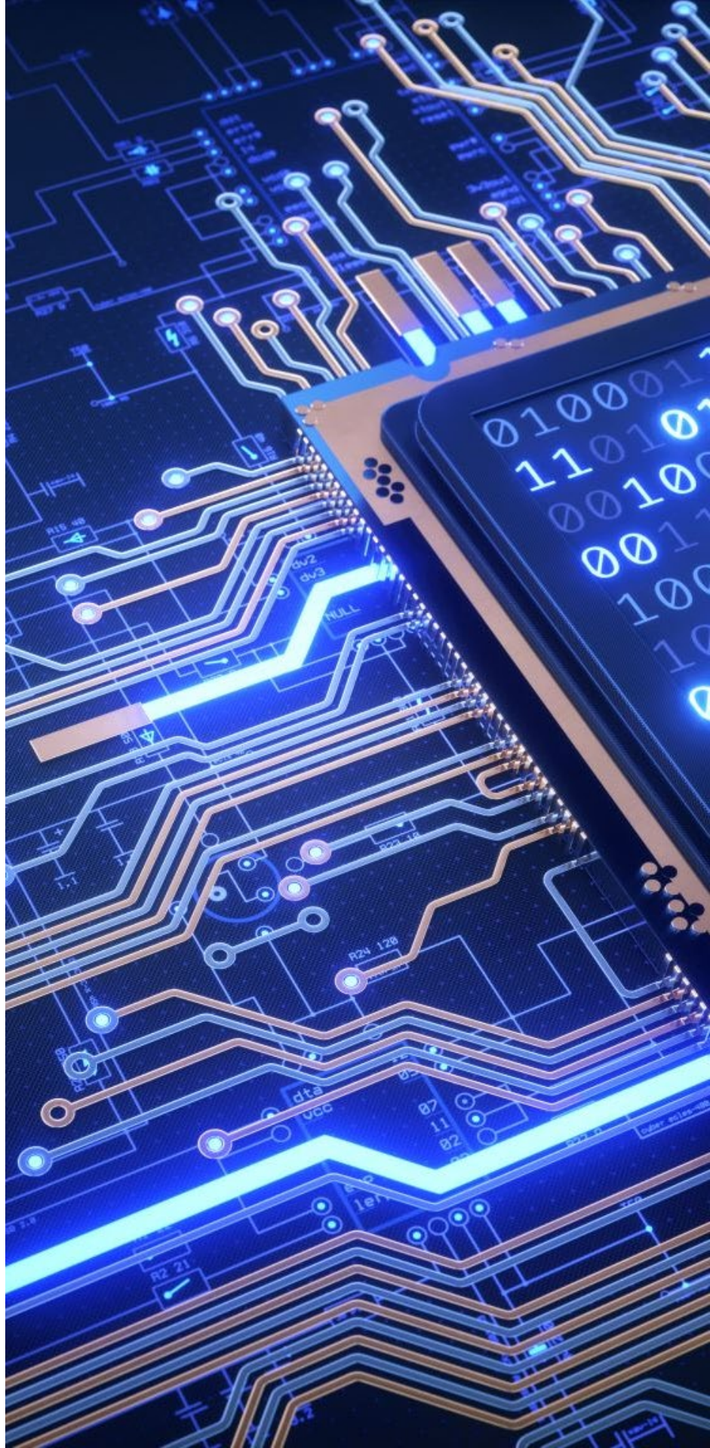
Governance Requirements [Section 500.4]

November 1, 2024

Cybersecurity Risk Management

Board or senior governing body oversight including:

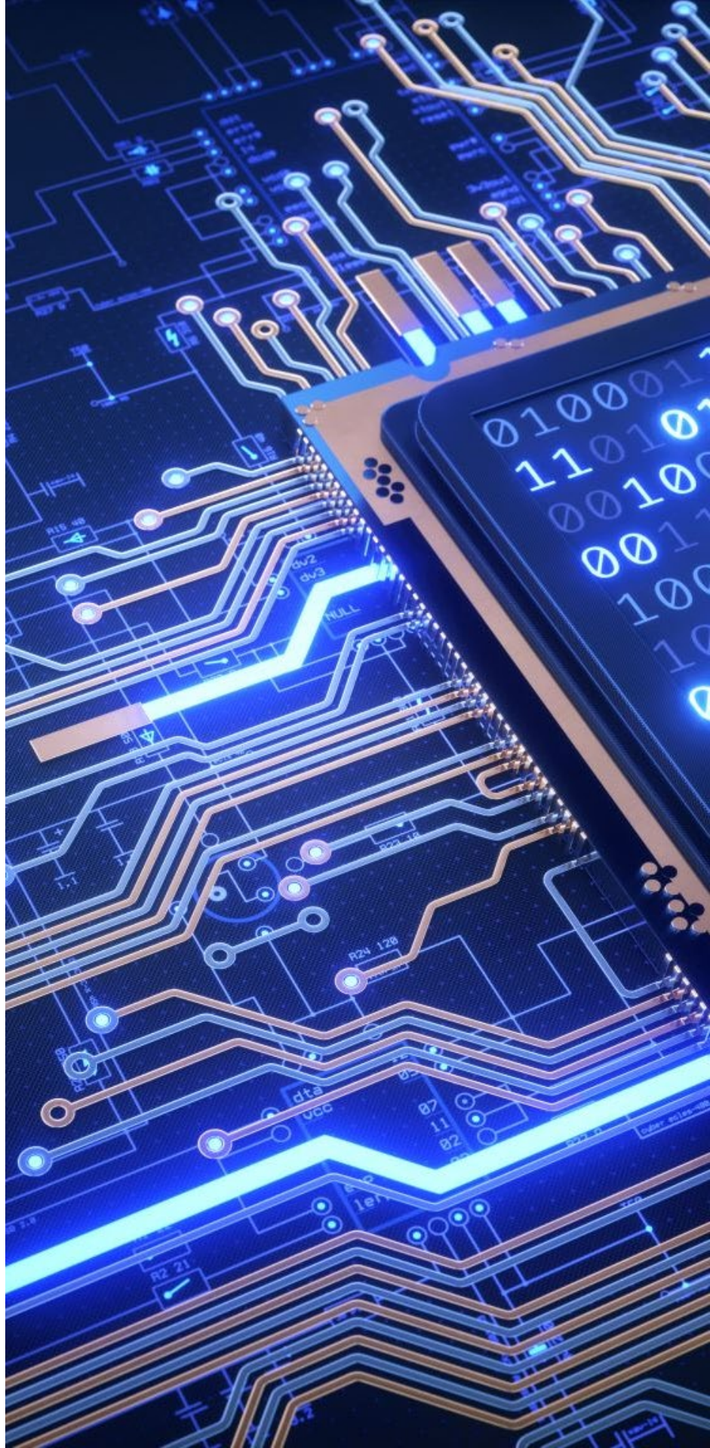
- “Having sufficient understanding of cybersecurity-related matters to exercise such oversight, which may include the use of advisors”
- “Requiring the covered entity’s executive management or its designees to develop, implement and maintain the covered entity’s cybersecurity program”
- “Regularly receiving and reviewing management reports about cybersecurity matters”
- “Confirming that the covered entity’s management has allocated sufficient resources to implement and maintain an effective cybersecurity program”



Incident Response [Section 500.16]

Existing Requirements for Incident Response Plan

- Internal processes for responding to a cybersecurity event
- Goals of the incident response plan
- 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 as necessary of the incident response plan following a cybersecurity event

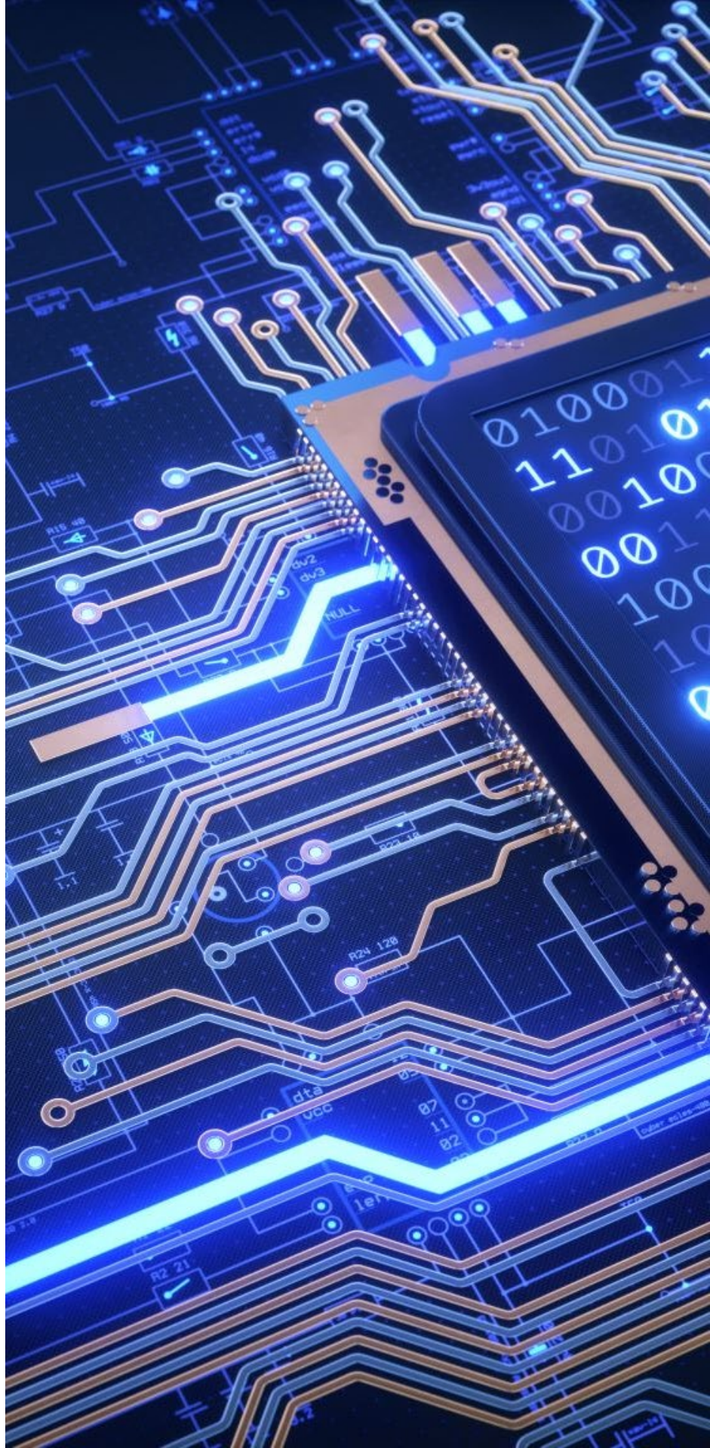


Incident Response [Section 500.16]

November 1, 2024

Update Plans to Address

- Recovery from backups
- Update incident response plans as necessary
- Train all employees involved in plan implementation
- Test plans with critical staff
- Test the ability to restore critical data and information systems from backups
- Maintain and adequately protect backups necessary to restore material operations

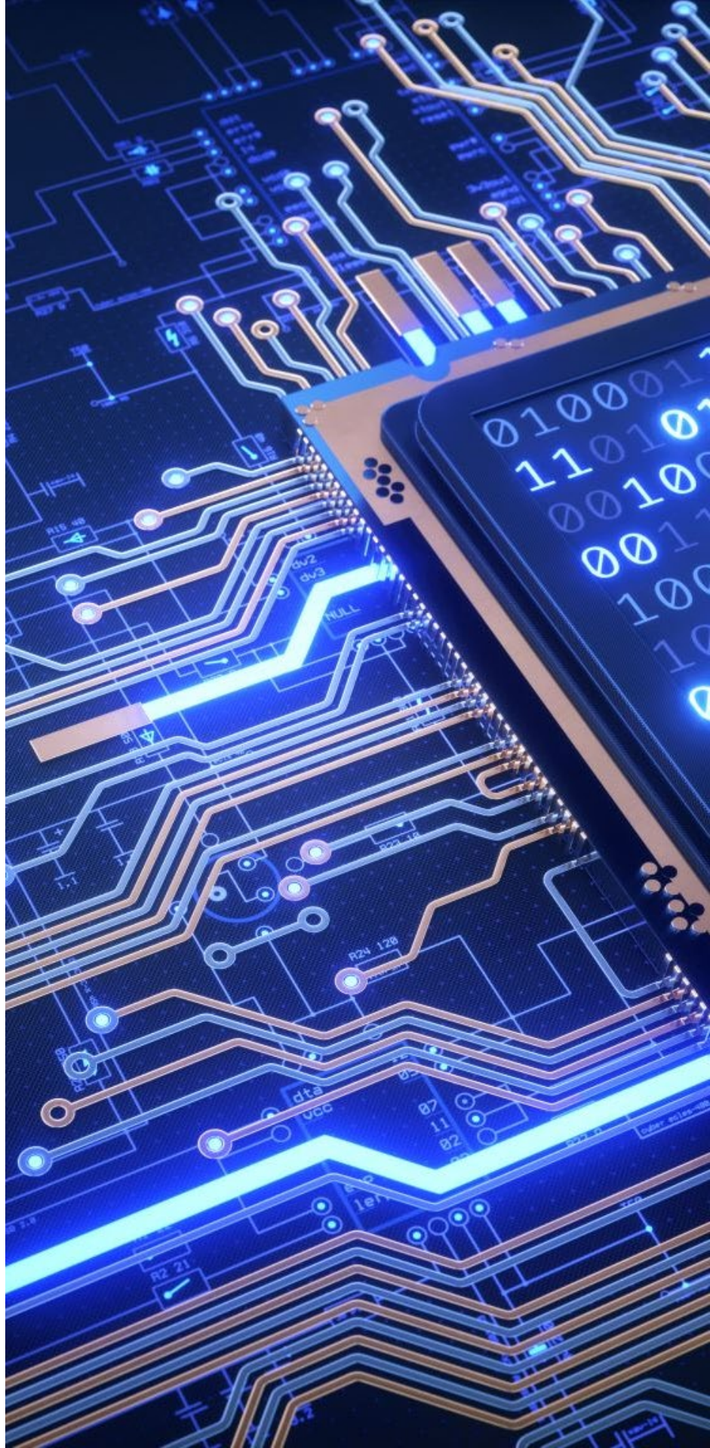


Incident Response [Section 500.16]

November 1, 2024

Business Continuity & Disaster Recovery (BCDR) Plan

- Identify documents, data, facilities, infrastructure, services, personnel and competencies essential to the continued operations of the covered entity's business
- Identify the supervisory personnel responsible for implementing each aspect of the BCDR plan
- Include a plan to communicate with essential persons in the event of a cybersecurity-related disruption
- Include procedures for the timely recovery of critical data and information systems and to resume operations as soon as reasonably possible
- Include procedures for backing up or copying, with sufficient frequency, information essential to the operations of the covered entity and storing such information offsite
- Identify third parties that are necessary to the continued operations of the covered entity's information systems.



Encryption [Section 500.15]

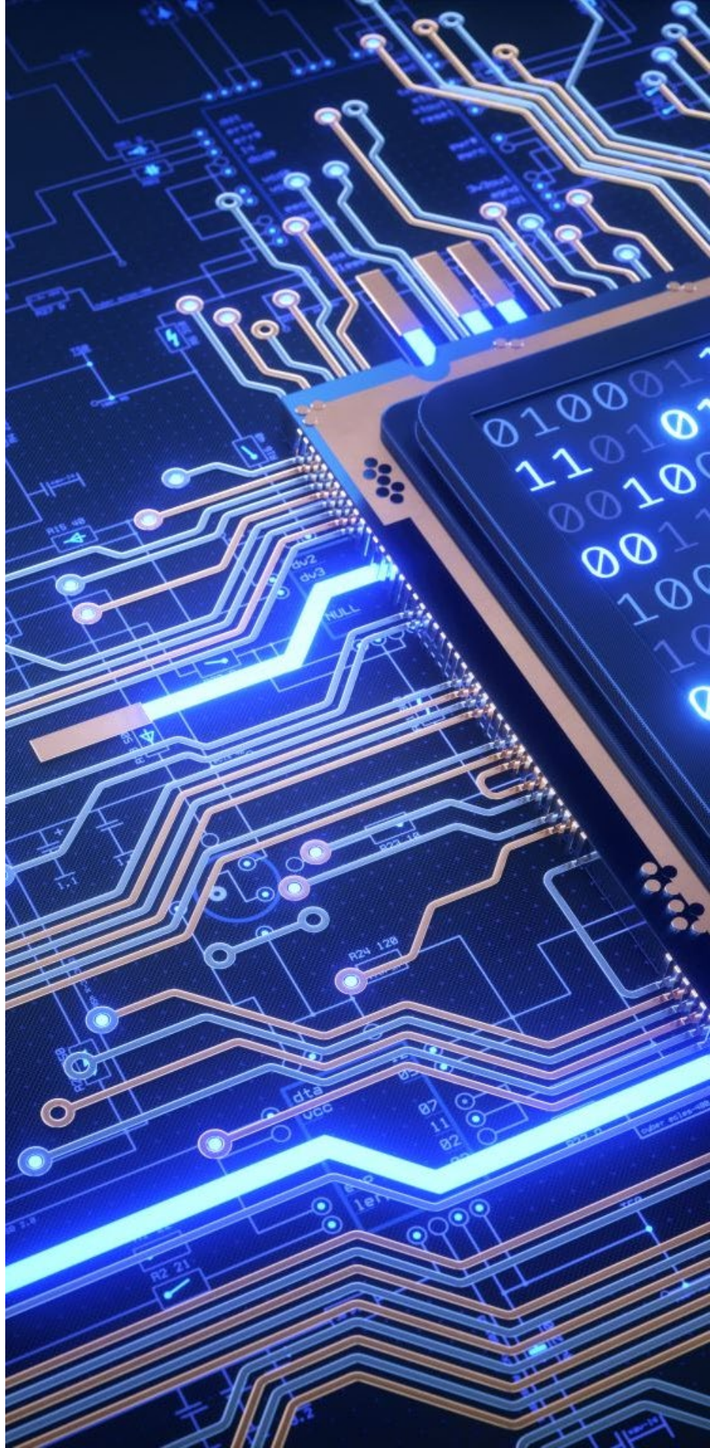
November 1, 2024

Stricter encryption requirements

- Requires industry standard encryption to protect nonpublic information both in transit over external networks and at rest

CISO approval of exceptions

- If a covered entity determines encryption is infeasible, the CISO review alterative controls and approve in writing
- The CISO must review the alternative controls at least annually



pillsbury

Checklist & Investigation Best Practices

Key Considerations in Responding to a Cybersecurity Event

pillsbury

NY DFS Cybersecurity Regulation

Incident Response and Notification Checklist

In responding to a Cybersecurity Incident and determining security and notification issues, consider the following steps:

1. Did a "Cybersecurity Incident" occur?

- Have you notified another government or regulatory agency (such as a state attorney general or the SEC, FTC, HHS Office for Civil Rights)?
- Does the incident have "a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity"?

4. Attorney Client Privilege

As soon as a potential cybersecurity incident is anticipated, confirm legal protections are in place to receive legal guidance on cyber investigation, notification, regulatory inquires and potential litigation.

5. Insurance Coverage

- Is the Cybersecurity Incident covered by insurance?

Key Considerations in Responding to a Cybersecurity Event

Legal protections in place for investigation and guidance

- Often overlooked in initial response
- Attorney client privilege
- Work product

Forensic assessment

- Are specialists tailored to the needs and incident?
- Determine scope and circumstances
- Remediation issues

Key Considerations in Responding to a Cybersecurity Event

Incident Response and BCDR Plans

- Managing external and internal communications and information sharing
- Identify backup data that has not been impacted by the incident

Containing the Incident and Restoring Security

- Determine attack vector and cause
- Appropriate security steps
    - Disable user accounts, install patches, change passwords, tailored to circumstances

Key Considerations in Responding to a Cybersecurity Event

Law Enforcement Referrals

- In appropriate cases, is there sufficient evidence for criminal enforcement?
- Jurisdiction
- Forensically imaged copies of data

pillsbury

Other Key Issues

Cybersecurity Events

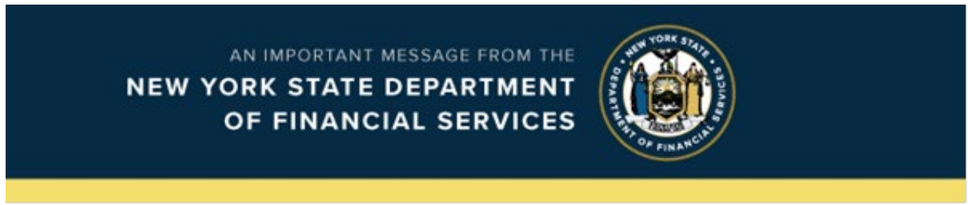
"any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such information system." [Section 500.1(f)]

Cybersecurity Events: Range of Threat

- Phishing
- Ransomware
- Business email compromise
- Cyber fraud
- Insider threats
- Nation state attacks
- Targeted or malicious attacks
- Attacks by former employees
- Employee inadvertence
- Supply chain issues
- Third party vendors
- Among others

NYDFS Security Risks & Announcements

September 27, 2024



Cybersecurity Threat Alert: Social Engineering of Institutions' IT Help Desk Personnel

- Targeting IT help desks and call centers
- DFS-regulated entities should be on high alert for suspicious phone communications
- Implement controls to prevent changing of passwords or intercepting of messaging applications to obtain MFA
- Diligent authentication of callers' identities

Notification Requirements

Notification [Section 500.17(a)]

- "in no event later than 72 hours after determining that a cybersecurity incident has occurred at the covered entity, its affiliates, or a third-party service provider."

Cybersecurity Incident

1. impacts the covered entity and requires the covered entity to notify any government body, self-regulatory agency or any other supervisory body;
2. has a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity; or
3. results in the deployment of ransomware within a material part of the covered entity's information systems.

New Requirement to Report Ransomware Payments

Extortion Payment Notifications [Section 500.17(c)]

- If a ransomware payment is made, notify DFS within 24 hours of payment
- Within 30 days of payment, provide all the reasons payment was necessary, alternatives to payment that were considered and the diligence, or research, in considering alternatives
- Describe the compliance with all applicable rules and regulations including those of the Office of Foreign Assets Control

pillsbury

Legal Issues & Services

Legal Issues & Services

Are you prepared for an examination?

- DFS examination process
- Record requirements
  - Maintain records “for examination and inspection” supporting Certification of Material Compliance or Acknowledgement of Noncompliance [Section 500.17(b)(1)]
- Penalty assessment factor
  - “whether the violation was a result of failure to remedy previous examination matters requiring attention, or failing to adhere to any disciplinary letter, letter of instructions or similar” [Section 500.20(c)]

Legal Issues & Services

Notifications

- Legal and forensic considerations
  - "reasonable likelihood of **materially harming** any **material part** of the normal operation(s)"
- Managing multiple notifications?
- Sufficiency of the notification

Annual Certification of Material Compliance or Acknowledgement of Noncompliance

- Internal review process in advance of April 15

Legal Issues & Services

Training

- Designing a compliant training program
- Ensure training is carried out effectively

Governance review

- How is cyber risk managed?
- Effective oversight by board
- Role and authority of CISO

Legal Issues & Services

Cyber Insurance Review

	Coverage	Description
1st Party Costs	Business Income/Extra Expense	Reimbursement for loss of income and/or extra expense resulting from an interruption of computer systems due to a network security breach.
	Data Asset Protection	Recovery of costs and expenses to restore, recreate, or recollect your data and other intangible assets that are corrupted or destroyed by a computer attack
	Cyber Extortion	The costs of consultants and extortion monies for threats related to interrupting systems and releasing private information
3rd Party Costs	Breach Response	The costs of complying with the various breach notification laws and regulations, legal expenses, call centers, monitoring, forensic services, and public relations
	Privacy Liability	Defense and liability for the failure to prevent unauthorized access, disclosure or collection of confidential information.
	Network Security Liability	Defense and liability for failure of system security to prevent or mitigate a cyber attack.
	Privacy Regulatory Defense	Costs to defend an action or investigation by regulator due to a privacy breach, including indemnification for any fines or penalties assessed
	Media Liability	Defense and liability for online libel, slander, misappropriation of name or likeness, plagiarism, copyright infringement, disparagement, negligence in content

Legal Issues & Services

Regulatory

- Investigative inquiries
- Multiple jurisdictions

Litigation

- Class Actions
- Indemnification
- Computer Fraud and Abuse Act
- Arbitration or mediation options

pillsbury

Questions

Mark L. Krotoski

Partner
Litigation

Full Biography

+1.650.233.4021
mark.krotoski@pillsburylaw.com

A Litigation partner who leads the firm's Cyber Disputes and Cartel Enforcement teams, Mark has more than 25 years' experience handling cybersecurity cases, investigations and issues.

Mark assists clients on cyber litigation and disputes, responding to data breaches, cyber incidents, misappropriation of trade secrets, conducting confidential cybersecurity investigations, mitigating and remediating cyber risks, developing cybersecurity protection plans, responding to regulatory investigations, and coordinating with law enforcement on cyber crime issues.

At DOJ, he prosecuted and investigated nearly every type of international and domestic computer intrusion, cybercrime, economic espionage, trade secret, and criminal intellectual property cases.

Mark served as the national coordinator for the Computer Hacking and Intellectual Property (CHIP) Program in the DOJ's Criminal Division, and as a cyber crime prosecutor in Silicon Valley, among other DOJ leadership positions.

Representative Experience

- Represented companies in complying with standards under the New York Department of Financial Services Cybersecurity Regulation.
- In representing an international retail company, led the forensic investigation concerning a cyberattack involving the acquisition of millions of customer records in all U.S. jurisdictions and more than 100 countries, provided guidance on legal obligations and coordinated with law enforcement, resulting in the identification and conviction of the perpetrator outside the United States.
- Represents clients on cyberattacks and violations of the Computer Fraud and Abuse Act including data breach class action cases.
- In the Yahoo data breach involving "at least 500 million" stolen user accounts, represented the manager of incident response during all phases of the investigation by the Department of Justice, Securities and Exchange Commission and Special Committee.
- Represented numerous companies in responding to ransomware and other cyberattacks, including through all phases involving the internal forensic investigation under attorney client privilege, review of data to determine notification requirements, notifications to federal and state regulators, responding to federal and state regulatory investigations, and follow-on litigation.
- Represented numerous international and domestic companies during investigations of cyber fraud and unauthorized wire transfers (referred to as a "business email compromise").
- Represented multiple companies in cyber risk assessments during an acquisition of or merger with another company.
- Lead counsel in a jury trial resulting in the conviction related to the intrusion into the Yahoo account of Alaska Governor Sarah Palin and obstruction of justice. Successfully argued the appeal before the U.S. Court of Appeals for the Sixth Circuit, affirming conviction.
- Lead counsel in a jury trial conviction of a system administrator who planted a "time bomb" on the company network after his departure.

Brian H. Montgomery

Senior Counsel
Financial Industry Group

Full Biography
+1.212.858.1238
brian.montgomery@pillsburylaw.com

Brian Montgomery utilizes his background in consumer protection and financial services regulation to strategically advise businesses on state and federal regulatory compliance.

Brian represents and advises banks, non-bank financial institutions, fintech companies, money services businesses and other businesses on regulatory and compliance matters, with a focus on consumer financial products and services. He advises companies on how to navigate regulatory issues as they bring innovative financial products and services to market. Brian also counsels clients on compliance with regulators' cybersecurity, IT and third-party risk management requirements.

Prior to joining the firm, Brian served in several senior positions at the New York Department of Financial Services, including leading the department's program to examine regulated institutions for compliance with federal and state consumer financial laws. Brian also supervised a group that conducted investigations and brought enforcement actions involving consumer financial products and services.

Representative Experience

- Advising financial institutions on U.S. financial services regulators' cybersecurity regulations and guidance.
- Supervised investigation of a significant data breach at a financial institution, resulting in a consent order.
- Representing several commercial banks in development and roll-out of nationwide digital banking platforms, including regulatory and related issues.
- As deputy superintendent at the NYDFS, oversaw consumer compliance and fair lending examinations of banks, non-depository lenders, loan servicers, credit reporting agencies and other regulated institutions, as well as Community Reinvestment Act examinations.
- Advising several consumer and commercial lenders on regulatory requirements for lending programs, including startup and ongoing compliance.
- Advising banks on compliance with Office of the Comptroller of the Currency (OCC) and Federal Financial Institutions Examination Council (FFIEC) requirements for third-party risk management and technology service providers.
- Provided guidance, in conjunction with Tokyo-based law firm, City-Yuwa, to the Japanese Financial Services Agency (FSA) regarding how to appropriately regulate the trading of stablecoins, a digital currency attached to a stable reserve asset, in Japan under the country's amended Payment Services Act.
- Served on the Virtual Currency Licensing Committee at the New York Department of Financial Services.
- Brought first action by state banking regulator under Title X of Dodd-Frank, the Consumer Financial Protection Act, resulting in consent judgment with auto lender and its president.
- Core member of the team that drafted the New York Financial Services Law and associated legislation that created the NYDFS by merging the banking and insurance departments. Subsequently planned and coordinated the merger of the consumer protection functions of the former departments.