FIRST PARTY SUMMIT
COLLECTIONS . CARE . OUTSOURCING
PRESENTED BY insideARM

Cyber Risk Management in 2017

Jonathan D. Klein, Esq., Attorney – Clark Hill PLC

Kia D. Floyd, Director of State Government Affairs – RELX, Inc.

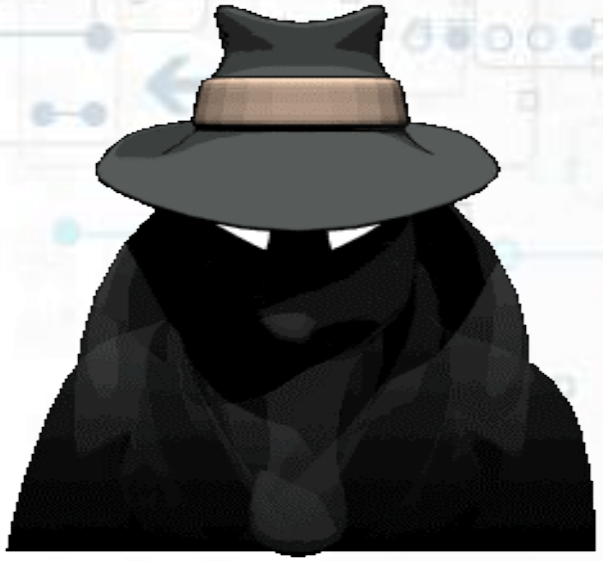
Bonus Track *Sponsored by* LexisNexis® RISK SOLUTIONS

"I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."

FBI Director Robert Mueller
RSA Cybersecurity Conference
March 2012

Threat Actors

- Cybercriminals
- Hackers
- Hactivists
- Government surveillance
- State sponsored / condoned espionage
- Insiders (disgruntled / dishonest / bored / untrained)



What are the Threat Actors After?

- Money
- Personally Identifiable Information
- Intellectual Property
- Trade Secrets
- Information on Litigation/Transactions
- Computing Power
- National Security Data
- Denial/Disruption of Service

Cybersecurity Regulation by the Numbers

Industry-Specific Security Regulations:

Gramm-Leach-Bliley Act (GLB)

Health Insurance Portability and Accountability Act (HIPPA)

Family Educational Rights and Privacy Act (FERPA)

Payment Card Industry Data Security Standards (PCI-DSS)

Federal Information Security Management Act (FISMA)

IRS Publication 1075 (IRS)

Department of Defense Guidelines (DoD)

Federal Cybersecurity Regulators:

Federal Trade Commission (FTC)

Federal Deposit Insurance Corporation (FDIC)

Federal Bureau of Investigation (FBI)

Office of the Comptroller of the Currency (OCC)

Securities and Exchange Commission (SEC)

Financial Industry Regulatory Authority (FINRA)

U.S. Department of Defense (DoD)

State Security Breach Regulations:

48 States + DC, Guam, Puerto Rico, and Virgin Islands

Only 2 States Do Not: Alabama and South Dakota

State Cybersecurity Regulations

Massachusetts

New York

Gramm-Leach-Bliley Financial Modernization Act

- Passed in 1999 to address data privacy and security by establishing standards for safeguarding customers' "nonpublic personal information," or personally identifiable financial information, stored by "financial institutions."
- Two primary sets of regulations:
  1. Interagency Guidelines (U.S. Department of Treasury); and
  2. Safeguards Rule (Federal Trade Commission)
- Requires financial institutions to:
  1. Provide notice of information-sharing practices to customers; and
  2. Safeguard sensitive data
- Enforcement?

Office of the Comptroller of the Currency (1/2)

- Until recent years, provided limited practical guidance for how financial institutions can live up to regulatory expectations for data security.
- Now examiners will use a Cyber Security Assessment Tool to determine a bank's ability to detect, prevent, and respond to cyber threats. The Tool provides two levels of assessment.
- First, it contains five (5) criteria for banks to evaluate their inherent risk profile:
  - ✓Technologies and Connection Types;
  - ✓Delivery Channels;
  - ✓Online/Mobile Products and Technology Services;
  - ✓Organizational Characteristics; and
  - ✓External Threats.

Office of the Comptroller of the Currency (2/2)

- Second, after determining its inherent risk profile, an institution uses the second level to determine the institution's level of "maturity" for cybersecurity preparedness within each of the following five (5) areas:
  - ✓Cyber Risk Management and Oversight;
  - ✓Threat Intelligence and Collaboration;
  - ✓Cybersecurity Controls;
  - ✓External Dependency Management; and
  - ✓Cyber Incident Management and Resilience.
- The OCC does not provide further guidance on what role the Tool will play in the results of its examinations, nor what examiners will be looking for in a bank's own analysis of its systems within the Tool's parameters.

Federal Deposit Insurance Corporation (FDIC)

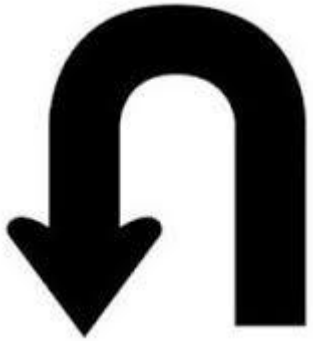
- FDIC works with financial institutions to help protect customer information/money.
- Since 2001, federal law and regulations require that financial institutions have programs to ensure security and confidentiality of customer information. Federal and state bank examiners also regularly conduct on-site examinations of FDIC-insured institutions and their outside firms to ensure compliance. Banking regulators also work with institutions to share overviews of the cyber-threat landscape and discuss steps they can take to be prepared.
- For example, in 2015, the FDIC produced an educational video on cybersecurity to help boards of directors and senior management at banks protect against potential threats. That same year, the regulators unveiled a voluntary "cybersecurity assessment tool" to help institutions identify risks and assess their preparedness.

State of Cybersecurity in 2017: The Big Shift

Mid-1990s to Late-2016: Broad, flexible approach to cybersecurity

Late-2016 to Present: Shift to specific requirements for cybersecurity

Why the sudden shift in cybersecurity regulation?



Causes of Shift to Specific Requirements

- Federal legislation on cybersecurity is hard to pass;
- Key concern for state and local governments;
- Better understanding of steps to protect against cyberattacks;
- Multitude of differing and divergent cybersecurity frameworks and regulations;
- Collaboration among various agencies; and
- State governments also have taken sincere measures to improve cyber security by increasing public visibility of firms with weak security.

Trump and Cybersecurity: The Great Conflict

President Trump's statements on regulation in general indicate a strong desire for de-regulation. In fact, shortly after taking office, President Trump told a group of business leaders that he intended to cut federal regulations by 75%. What does this mean for cybersecurity regulations?

Maybe Nothing... Why not?

In stark contrast, President Trump appears to want to strengthen the country's cybersecurity efforts. The President has stated that cybersecurity is an immediate priority of his administration. How he accomplishes that goal remains to be seen. Indeed, to date, the Trump Administration has not yet settled on a comprehensive cybersecurity policy.

Forecast Under the Trump Administration

- Trump could focus on removing some of the bureaucracy under which the financial services industry operates by working towards a single entity managing the requirements → January 30, 2017 Executive Order
- De-regulate the cybersecurity industry → What happens if that occurs?
- Consolidate cybersecurity regulations
- “Public-private” partnerships + other incentives > mandatory regulations
- “Positive incentives” (e.g., tax breaks) to encourage cybersecurity

FIRST PARTY SUMMIT
COLLECTIONS . CARE . OUTSOURCING
PRESENTED BY insideARM

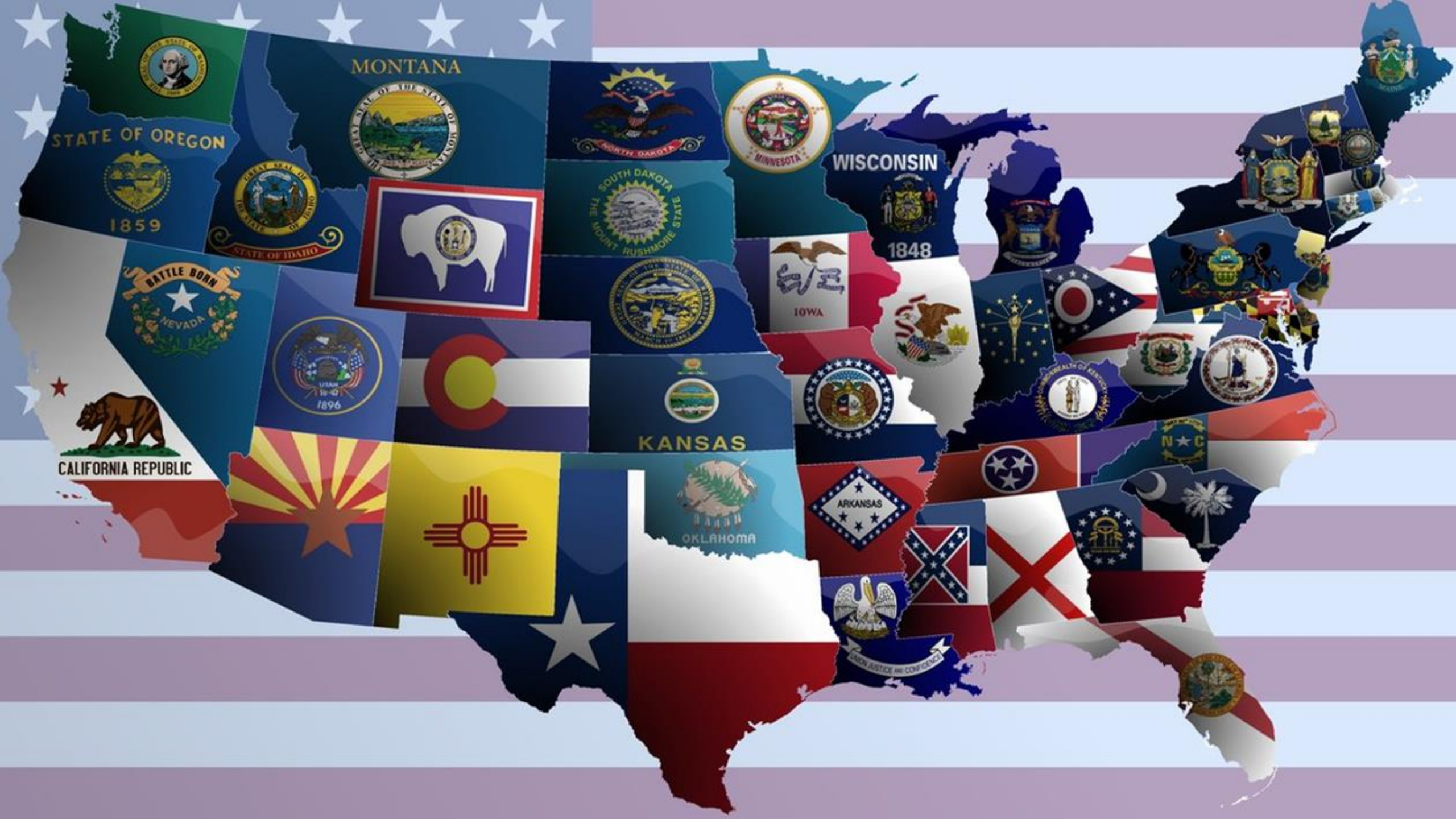
The State of the States on Cybersecurity Policy

What to Expect from State Regulators

2017 and beyond

Bonus Track *Sponsored by*

LexisNexis®
RISK SOLUTIONS


MONTANA
STATE OF OREGON
1859
STATE OF IDAHO
NORTH DAKOTA
SOUTH DAKOTA
THE MOUNT RUSHMORE STATE
MINNESOTA
WISCONSIN
1848
IOWA
BATTLE BORN
NEVADA
UTAH
1896
KANSAS
CALIFORNIA REPUBLIC
OKLAHOMA
ARKANSAS
N C

Navigating the 50-State Patchwork of Laws

- The lack of a comprehensive federal cybersecurity standard has created a 50-state patchwork approach-- each state wants to craft its own laws.
- In 2016, 28 states considered cybersecurity legislation. Fifteen of those states enacted legislation addressing:
  - Data security practices and the protection of information in government agencies,
  - Exemptions from the state Freedom of Information Act for data affecting the security of critical infrastructure, and
  - Cybersecurity and computer crimes.

Federal vs. State Public Policy

Federal	State
Timing. Slow and deliberate. Passing legislation is like running a marathon.	**Timing.** Fast and often reactive. Passing state legislation is like running a sprint.
Motivation. Laws are prompted by constituents, interest groups, globalization, desire for uniform national standards and legacy issues.	**Motivation.** Laws are often spurred by a single constituent issue, isolated data breach, news/media, or in reaction to federal policy.
Implementation. Lawmaking is collaborative, considers compliance impacts and resources for implementation. Regulatory processes allow for public comment.	**Implementation.** Laws may be enacted quickly, without a full review of compliance impacts and implementation resources. No guaranteed regulatory process. As a result, effective dates are often delayed or extended.
Perspective. The U.S. government is usually aware of and considers its competitive, global position.	**Perspective.** States are more insular and parochial; they don't always consider multi-jurisdictional compliance or global competition.

The Challenges of State Cybersecurity Laws

- Delayed enactment of laws
  - Due to lack of in house expertise and knowledge of impacts
- Laws fall behind in context and time
  - Technology evolves rapidly and government struggles to keep pace
  - Today's technology may be obsolete tomorrow (ie, multi-factor authentication)
  - Prescriptive regulations stifle innovation
- Conflicts of laws and Limitations on the scope of application
  - Lack of understanding of limits on state sovereignty, federal pre-emption, industry best practices and corporate business structures

Data Security Today

- As states become more active in enacting data security and privacy policy, political motivations have become more pronounced.
- Privacy laws are often a convergence of progressive and conservative ideologies.
- In 2017 lawmakers have been explicit about being politically motivated.

FIRST PARTY SUMMIT
COLLECTIONS . CARE . OUTSOURCING
PRESENTED BY insideARM

NY Department of Financial Services (NYDFS) Regulation 23 NYCRR 500

A New Era of State Regulation

Bonus Track ***Sponsored by***

LexisNexis® RISK SOLUTIONS

NY Dept. of Financial Services Regulation 23 NYCRR 500

Understanding the Basics (Why, Who, What, When, What Next)

1. Why was it created?
2. Who does it impact?
3. What does it do?
4. When does it take effect?
5. What next?

NYDFS Scope of Authority

- The New York State Department of Financial Services (NYDFS) was created through a merger of the State Banking Department and the State Insurance Department on October 3, 2011.
- NYDFS governs state-chartered financial institutions, insurers, third party service providers and third party application providers (ie, technology contractors).
- NYDFS does not supervise national banks and federal branches of foreign banks but they do oversee state-licensed lenders and branches of foreign banks.

Why the NYDFS Regulations Were Created

NYDFS 23 NYCRR 500 is an omnibus set of cybersecurity regulations introduced in response to a series of high-profile data breaches which resulted in losses of hundreds of millions of dollars to U.S. companies, such including Target Corp., Home Depot, and Anthem Healthcare.

Covered Entities, Affiliates & 3rd Party Providers

- Section 500.01 Definitions.

*(a) **Affiliate** means any Person that controls, is controlled by or is under common control with another Person. For purposes of this subsection, control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise.*

*(c) **Covered Entity** means any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.*

*(n) **Third Party Service Provider(s)** means a Person that (i) is not an Affiliate of the Covered Entity, (ii) provides services to the Covered Entity, and (iii) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity.*

Examples of Covered Entities

- Banks & Trust Companies
- Budget Planners
- Charitable Foundations
- Check Cashers
- Credit Unions
- Domestic Representative Offices
- Foreign Agencies
- Foreign Bank Branches
- Foreign Representative Offices
- Health Insurers, Accident and Related Entities
- Holding Companies
- Investment Companies
- Licensed Lenders
- Life Insurance Companies
- Money Transmitters
- Mortgage Bankers
- Mortgage Brokers
- Mortgage Loan Originators
- Mortgage Loan Servicers
- New York State Regulated Corporations
- Premium Finance Agencies
- Private Bankers
- Property and Casualty Insurance Companies
- Safe Deposit Companies
- Sales Finance Companies
- Savings Banks and Savings and Loan Associations (S&Ls)
- Service Contract Providers

What Do the Regulations Require?

- The Regulations are divided into 16 timelines, 7 of which must be completed within 180 days of the effective date Mar. 1, 2017. (The others have start dates of 1 year, 18 months, or 2 years).
- A Cybersecurity Program: Companies must establish and maintain a cybersecurity program to protect sensitive information from unauthorized access, use, and malicious attacks.
  - The program must include a mechanism for data security breach detection, prevention and remediation. See § 500.02.

The Requirements- Cybersecurity Policy

- Policy: A written cybersecurity policy, reviewed annually by the board of directors and approved by a CISO or senior officer responsible for compliance. See § 500.03(b).
- The cybersecurity policy must address:
  - A description of current security measures in place to protect data infrastructure and customer data privacy;
  - Procedures to maintain, monitor, and update information systems and networks, including management of third-party service providers;
  - Assessments of the information systems' security risks and operations concerns; and
  - Procedures to respond and recover from security breaches.

The Requirements- Data Protection

- Encryption: Encryption of all nonpublic information in transit and at rest unless infeasible. See § 500.15.
- Multi-Factor Authentication: Employment of multi-factor and risk-based authentication for logging into information systems. See § 500.12.
- Application Security: Adoption of procedures (with annual reviews) for secure development practices for all applications developed in-house and assessment and security testing of all externally developed applications. See § 500.08.
- Third Party Information Security: Implementation of written policies and procedures regarding the security of the company's information systems and nonpublic information that are accessible by third parties doing business with the company. See § 500.11.

The Requirements- Accountability

- Personnel: Appointment of a CISO, responsible for:
  - Implementing the cybersecurity program and enforcing the cybersecurity policy, and
  - Employment of a cybersecurity team to manage the program and run the day-to-day cybersecurity functions.
  - Regular employee training on cybersecurity protocols. See §§ 500.04; 500.10.

- Data Retention Limitations: Policies and procedures for the timely destruction of any nonpublic information. See § 500.13.

The Requirements- Incident Response Plan

- Testing and Risk Assessment: The cybersecurity program must be tested to assess risks in its information systems. Testing must include a quarterly vulnerability assessment; an annual penetration test; and a formal risk assessment report which evaluates and categorizes identified risks. See §§ 500.05; 500.09.
- Incident Response Plan: Establish a written incident response plan designed to promptly respond to and recover from a cybersecurity breach. See § 500.16

When It Is Effective: Key Dates

- **March 1, 2017** – Regulation becomes effective. Covered entities must comply with all dates stated herein unless otherwise specified or exempted.
- **August 28, 2017** – 180-day transitional period ends.
- **September 27, 2017** – Initial 30-day period for filing Notices of Exemption ends.
- **February 15, 2018** – The First certification of compliance is due (on or prior to this date).
- **March 1, 2018** – 1-year transitional period ends. Must comply with certain requirements such as: penetration testing, vulnerability assessments, risk assessment and cybersecurity training.
- **September 3, 2018** – 18-month transitional period ends. Must comply with audit trail, data retention and encryption requirements.
- **March 1, 2019** – 2-year transitional period ends. Must develop a third-party service provider compliance program.

Lingering Questions Prompt FAQ's

The NYDFS has issued FAQs to address topics including:

- Whether a covered entity is required to give notice to consumers affected by a cybersecurity event;
- Whether a covered entity may adopt portions of an affiliate's cybersecurity program without adopting all of it;
- What constitutes "continuous monitoring" for purposes of the DFS Regulation;
- How a covered entity should submit Notices of Exemption, Certifications of Compliance and Notices of Cybersecurity Events; and
- Whether an entity can be both a covered entity and a third-party service provider.

What Next?

- While the NYDFS regulations were the first, they may not be the last.
- State lawmakers have become aggressive on privacy and some react to perceived and actual roll backs of federal privacy protections
- Today a CISO must be politically savvy and nimble in responding to state and federal regulation.
- Senior executives must be aware of the company enterprise vision, its threat response strategy, and the cybersecurity program to ensure that technologies are agile and assets are protected.
- State legislation moves quickly, but technology is still light years ahead of public policy.

Takeaways

- Stay informed of state public policy affecting financial services and debt collection. Leverage government affairs, legal and communications resources when needed.
- Review your incident security breach response plan and compensating controls.
- Prepare a narrative to defend your incident response and remediation ***before*** a security breach occurs.
- Test your program regularly. Run data security breach drills to review, test and assess program deficiencies
  - There is always a cybersecurity threat but it may not be the one you anticipate. A data breach doesn't end when you notify individuals regulators and customers.
- For more details on the NYDFS Regulations visit www.dfs.ny.gov

"We believe the best way for industry to focus on the threat of cybersecurity is to have a consistent framework. The New York regulation is a road map with rules of the road."

Maria Vullo, Superintendent of the New York Department of Financial Services,

Speaking to The National Association of Insurance Commissioners (NAIC)

April 2017