protiviti®

Face the Future with Confidence

CYBERSECURITY AND INTERNAL AUDIT'S ROLE

Dallas CPE Event--September 21, 2018

AGENDA

protiviti

Adam Hamm

Managing Director
Chicago, IL.

Direct: +312.476.6334
Mobile: +701.202.4442
E-Mail: **adam.hamm@protiviti.com**

Areas of Expertise

- Risk Management
- Compliance
- Cybersecurity
- Regulatory Relations
- Corporate Governance
- ORSA

Industry Expertise

- Insurance and Reinsurance
- Financial Services

Education & Certifications

- Bachelor of Science, Sam Houston State University
- Juris Doctorate, With Distinction, University of North Dakota School of Law
- Licensed Attorney

Professional Experience

Adam is a Managing Director with the global consulting firm Protiviti. He focuses on serving clients within the financial services industry concerning risk, compliance, and cybersecurity matters. He has deep knowledge of financial services regulation with hands on experience in all insurance supervision and policy related matters. Prior to joining Protiviti in January 2017, he was a former President of the National Association of Insurance Commissioners (NAIC), Chairman of the NAIC's Cybersecurity Task Force, Principal on the Financial and Banking Information Infrastructure Committee (FBIIC), Principal on the United States Financial Stability Oversight Council (FSOC) and North Dakota's elected insurance commissioner from 2007-2016. Adam also spent ten years as a violent crimes prosecutor and civil litigator.

Regulatory Experience

- In his most recent role with the NAIC, served as the Chairman of its National Cybersecurity Task Force where he spearheaded the development of a comprehensive insurance regulatory framework for cybersecurity in America. As Chairman of the Task Force, he testified before Congress on cyber issues and also served as a leader of the examination of Anthem following their 2015 data breach.
- Served as the insurance commissioner representative on FBIIC (America's cybersecurity regulatory committee for the financial services sector). FBIIC is chaired by the U.S. Treasury Department and is made up of the heads of all the major federal financial regulatory agencies. FBIIC's purpose is to help coordinate cybersecurity regulatory efforts in America's financial sector.
- Served as the insurance commissioner representative on FSOC, which was created from the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 to address matters of financial stability. FSOC is a fifteen member regulatory body where Adam served alongside America's chief financial regulators.
- Four years as an elected officer of the NAIC (2011-2014) culminating with serving as President of the NAIC in 2014. As an elected officer and President of the NAIC (an approximately 12,000 person organization), set insurance regulatory priorities for America's insurance regulators and oversaw the development of numerous regulatory initiatives, including cybersecurity, solvency modernization, ORSA, corporate governance, group supervision, and principles based reserving.
- As North Dakota's elected insurance commissioner from 2007-2016, oversaw a multi-billion dollar a year insurance market with more than 2,000 licensed insurance companies and 70,000 licensed insurance agents, served as President of North Dakota's high-risk health insurance pool, and served on North Dakota's State Investment Board overseeing approximately $11 billion in assets.

protiviti

ANTHEM DATA BREACH

- Background: data breach began in Feb. 2014 via a phishing e-mail; Anthem discovered the breach in Jan. 2015; approx. 80 million Americans affected, including approx. 12 million minors (all 50 states impacted); personal information taken included names, addresses, e-mail addresses, dates of birth, SSN's, medical ID's, employment information (including income data)

- Regulatory focus: Multistate exam of Anthem occurred following the data breach that was led by 7 states; focus of the exam centered on their pre-breach posture (how vulnerable were they), the adequacy of their response after the breach was discovered, and their post-breach corrective actions

- Primary concerns for regulators and key lessons learned: primary concerns were impacts to consumers and the long term impact to minors; key lessons learned revolved around the issues of network segmentation and breach detection

- Remediation issues: credit protection services to all impacted consumers for 2 years; credit freeze for all impacted minors; recovery from breach ultimately cost Anthem hundreds of millions of dollars

NYDFS PART 500 – CONTEXTUAL OVERVIEW

Regulation Background:

The New York State Department of Financial Services (NYDFS or DFS) **established a set of cybersecurity requirements, effective March 2017, for financial services companies who are supervised by the NYDFS to address the heightened risk of cyber attacks by nation-states, terrorist organizations, and independent criminal actors**. The regulation, Part 500 of Title 23 of the New York Code, aims to protect customer information as well as the information systems by holding *covered entities* accountable for their cyber defense responsibilities.

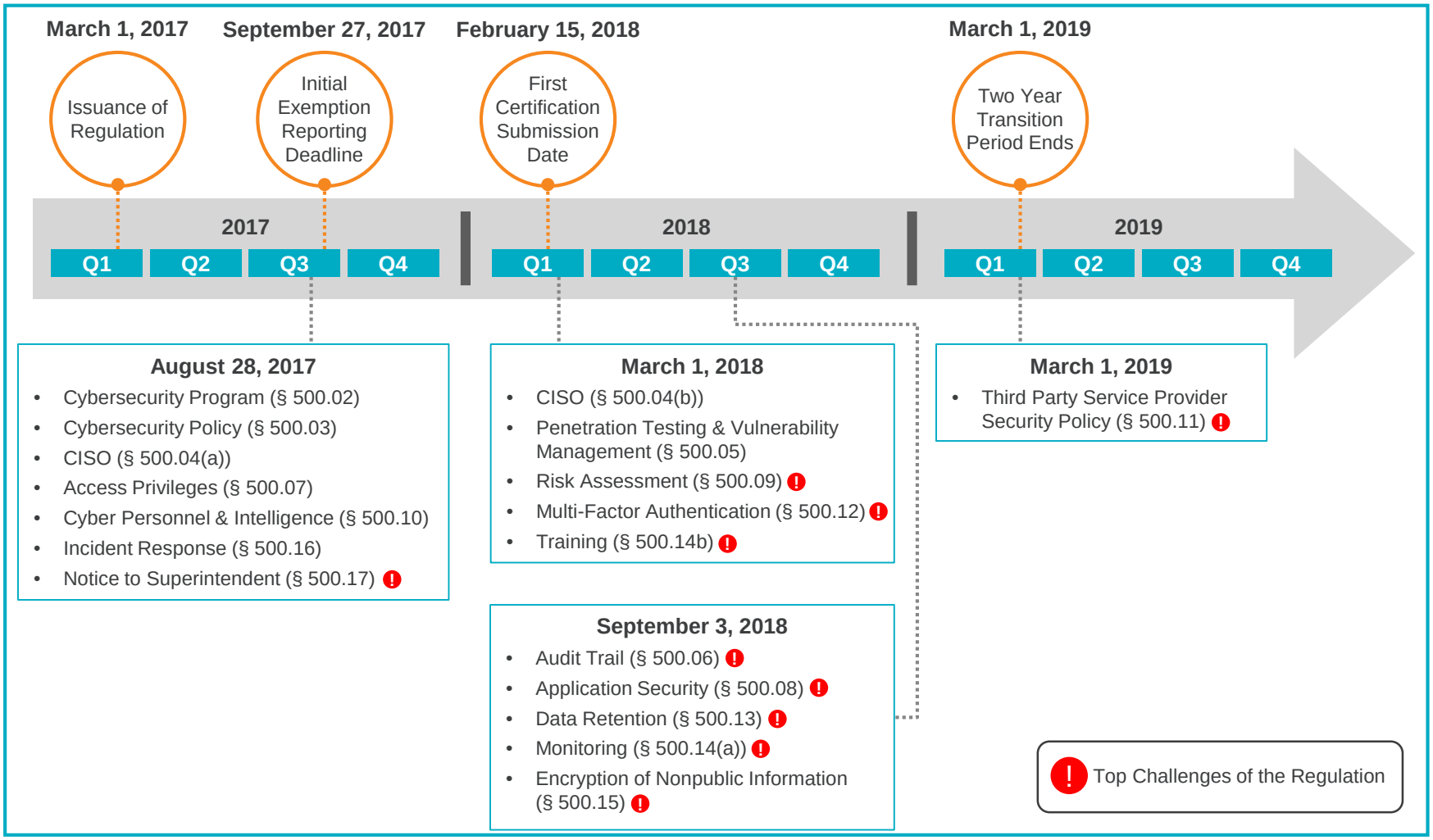
With the increase in threats to information and financial systems from all corners of the world, financial institutions are being closely monitored by regulators, including NYDFS.

Keeping the serious implications in view, **certain regulatory minimum standards are warranted, while not being overly prescriptive to keep pace with technological advances**. At a high level, the NYDFS Part 500 regulation requires each company to:

- Assess its specific risk profile and design a program that addresses its risks in a robust fashion;
- Design the cybersecurity program with senior management having full responsibility for the program and cybersecurity events;
- File an annual certification confirming compliance with the regulations; and,
- Ensure the entity's cybersecurity program supports the safety and soundness of the institution and protect its customers.

NYDFS PART 500 – TRANSITION PERIOD

NYDFS Part 500 is being rolled out through March 2019. The timeline below depicts when each portion of the regulation goes into effect.



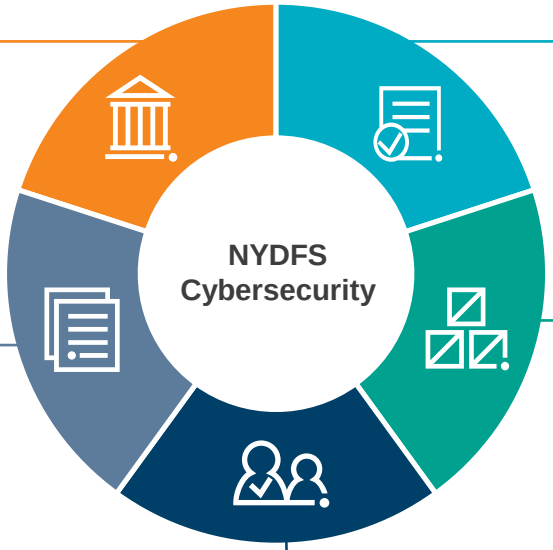
protiviti

KEY CONSIDERATIONS

How NYDFS Cybersecurity Impacts the Business

NYDFS cybersecurity regulations became effective March 1, 2017. Compliance will be phased-in with some requirements applying in 6 months and the last requirements due within 24 months.

The primary objective of the regulations is to help protect New York's financial services industry and consumers from the ever growing threat from cyber-attacks.



Governance

- Cybersecurity Program
- Board of Directors
- CISO
- Risk Assessments
- Policy and Standards
- Incident Response Plan

Reporting

- Annual Report to Board of Directors
- NYDFS – Annual Certification
- NYDFS – Cyber Event Reporting

Third Party Service Provider

- Risk Assessment
- Contract Clauses Due Diligence
- Periodic Assessments
- Policy
- Notice of Cyber Event

Testing & Assessments

- Penetration Testing
- Vulnerability Assessments
- Application Security
- Third Party Service Provider Testing

Technical Controls

- Access Controls and Access Privileges Review
- Encryption
- Multi-Factor Authentication
- Audit Trail Monitoring

protiviti

CYBERSECURITY PROGRAM §500.02

Effective 8/28/2017

Each Covered Entity shall maintain a **cybersecurity program** designed to protect the **confidentiality, integrity and availability** of the Covered Entity's Information Systems.

The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions:

- Identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems
- Use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.
- Detect Cybersecurity Events
- Respond to identified or detected Cybersecurity Events to mitigate any negative effects
- Recover from Cybersecurity Events and restore normal operations and services
- Fulfill applicable regulatory reporting obligations.

A Covered Entity may meet the requirement(s) by adopting the relevant and applicable provisions of a cybersecurity program maintained by an Affiliate, provided that such provisions satisfy the requirements set forth in the Third Party Service Provider Security Policy section. All documentation and information relevant to the Covered Entity's cybersecurity program shall be made available to the superintendent upon request.

CYBERSECURITY POLICY §500.03

Effective 8/28/2017

Each Covered Entity shall implement and maintain a **written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors** (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's **policies and procedures for the protection of its Information Systems and Nonpublic Information** stored on those Information Systems.

The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations:

- Information security
- Data governance and classification
- Asset inventory and device management
- Access controls and identity management
- Business continuity and disaster recovery planning and resources
- Systems operations and availability concerns
- Systems and network security
- Systems and network monitoring
- Systems and application development and quality assurance
- Physical security and environmental controls
- Customer data privacy
- Vendor and Third Party Service Provider management
- Risk assessment
- Incident response

CHIEF INFORMATION SECURITY OFFICER §500.04(a)

Effective 8/28/2017

Each Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy. **The CISO may be employed by the Covered Entity, one of its Affiliates or a Third Party Service Provider.**

The CISO shall consider to the extent applicable:

- The confidentiality of Nonpublic Information and the integrity and security of the Covered Entity's Information Systems
- The Covered Entity's cybersecurity policies and procedures
- Material cybersecurity risks to the Covered Entity
- Overall effectiveness of the Covered Entity's cybersecurity program
- Material Cybersecurity Events involving the Covered Entity during the time period addressed by the report

CHIEF INFORMATION SECURITY OFFICER §500.04(b)

Effective 3/1/2018

The CISO of each Covered Entity shall report in writing at least annually to the Covered Entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a Senior Officer of the Covered Entity responsible for the Covered Entity's cybersecurity program. The CISO shall report on the Covered Entity's cybersecurity program and material cybersecurity risks.

PENETRATION TESTING & VULNERABILITY ASSESSMENTS §500.05 *Effective 3/1/2018*

The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity's Risk Assessment, designed to **assess the effectiveness of the Covered Entity's cybersecurity program.** The monitoring and testing shall include continuous monitoring or periodic Penetration Testing and vulnerability assessments.

Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct:

- Annual Penetration Testing of the Covered Entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment
- Bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems based on the Risk Assessment.

AUDIT TRAIL §500.06

Effective 9/3/2018

Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment:

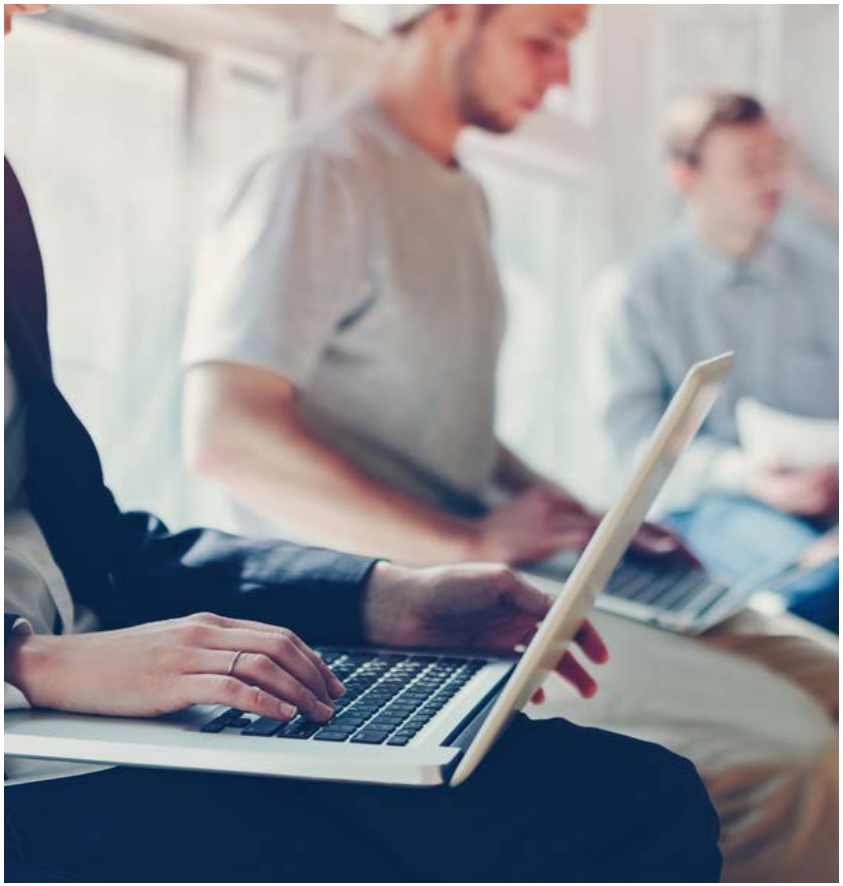
- Are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity
- Include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity

Each Covered Entity shall maintain records required by the first point of the above section for not fewer than five years and shall maintain records required by the second point of the above section for not fewer than three years.

ACCESS PRIVELEGES §500.07

Effective 8/28/2017

As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity **shall limit user access privileges to Information Systems that provide access to Nonpublic Information** and shall periodically review such access privileges.



APPLICATION SECURITY §500.08

Effective 9/3/2018

Each Covered Entity's cybersecurity program shall include **written procedures, guidelines and standards designed to ensure the use of secure development** practices for in-house developed applications utilized by the Covered Entity, and procedures for **evaluating, assessing or testing the security of externally developed applications** utilized by the Covered Entity within the context of the Covered Entity's technology environment.

All such procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the Covered Entity.

protiviti

RISK ASSESSMENT §500.09

Effective 3/1/2018

Each Covered Entity shall conduct a periodic Risk Assessment of the Covered Entity's Information Systems sufficient to **inform the design of the cybersecurity program** as required by this section. Such Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations. The Covered Entity's Risk Assessment shall allow for **revision of controls to respond to technological developments and evolving threats** and shall consider the particular risks of the Covered Entity's business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems.

The Risk Assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include:

- Criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity
- Criteria for the assessment of the confidentiality, integrity, security and availability of the Covered Entity's Information Systems and Nonpublic Information, including the adequacy of existing controls in the context of identified risks
- Requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.

CYBERSECURITY PERSONNEL & INTELLIGENCE

§500.10

Effective 8/28/2017

In addition to the requirements set forth in the CISO section, each Covered Entity shall:

- Utilize qualified cybersecurity personnel of the Covered Entity, an Affiliate or a Third Party Service Provider sufficient to manage the Covered Entity's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in the Cybersecurity Program section
- Provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks
- Verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

A Covered Entity may choose to utilize an Affiliate or qualified Third Party Service Provider to assist in complying with these requirements, subject to the requirements set forth in the Third Party Service Provider Security Policy section.

THIRD PARTY SERVICE PROVIDER SECURITY POLICY §500.11 *Effective 3/1/2019*

Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address to the extent applicable:

- The identification and risk assessment of Third Party Service Providers
- Minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity
- Due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers
- Periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices

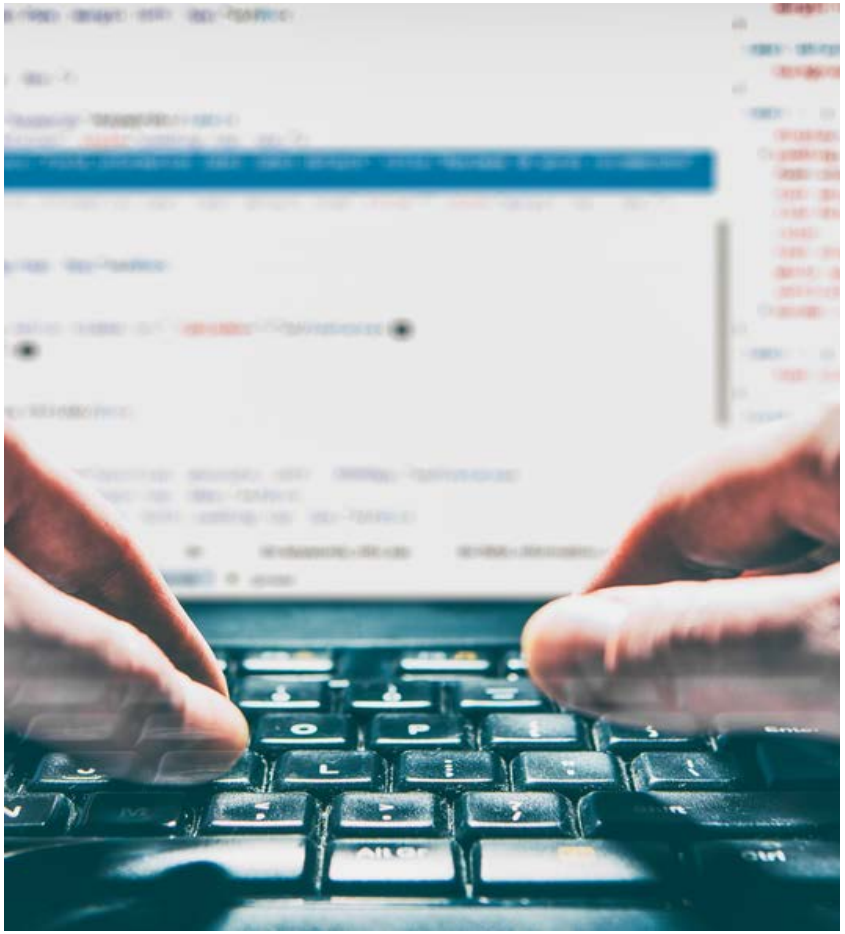
Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers including to the extent applicable guidelines

- The Third Party Service Provider's policies and procedures for access controls, including its use of Multi-Factor Authentication as required by the MFA Section, to limit access to relevant Information Systems and Nonpublic Information
- The Third Party Service Provider's policies and procedures for use of encryption as required by the encryption section to protect Nonpublic Information in transit and at rest
- Notice to be provided to the Covered Entity in the event of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or the Covered Entity's Nonpublic Information being held by the Third Party Service Provider
- Representations and warranties addressing the Third Party Service Provider's cybersecurity policies and procedures that relate to the security of the Covered Entity's Information Systems or Nonpublic Information.
  - Limited Exception: 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 regulation.

MULTI-FACTOR AUTHENTICATION §500.12

Effective 3/1/2018

Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include **Multi-Factor Authentication or Risk-Based Authentication**, to protect against unauthorized access to Nonpublic Information or Information Systems. Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, **unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.**



LIMITATIONS ON DATA RETENTION §500.13

Effective 9/3/2018

As part of its cybersecurity program, each Covered Entity shall include **policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information** identified in the definitions section that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity, **except where such information is otherwise required to be retained by law or regulation**, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

TRAINING AND MONITORING §500.14(a)

Effective 9/3/2018

As part of its cybersecurity program, each Covered Entity shall:

- Implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users

TRAINING AND MONITORING §500.14(b)

Effective 3/1/2018

As part of its cybersecurity program, each Covered Entity shall:

- Provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.

ENCRYPTION OF NONPUBLIC INFORMATION §500.15

Effective 9/3/2018

As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.

- To the extent a Covered Entity determines that encryption of Nonpublic Information in transit over external networks is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.
- To the extent a Covered Entity determines that encryption of Nonpublic Information at rest is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

To the extent that a Covered Entity is utilizing compensating controls under the above, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.

INCIDENT RESPONSE PLAN §500.16

Effective 8/28/2017

As part of its cybersecurity program, each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations. Such incident response plan shall address the following areas:

- The internal processes for responding to a Cybersecurity Event
- The goals of the incident response plan
- The 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
- The evaluation and revision as necessary of the incident response plan following a Cybersecurity Event

NOTICES TO SUPERINTENDENT §500.17

Effective 8/28/2017

Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following:

- Cybersecurity Event impacting the Covered Entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body
- Cybersecurity Event that has a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

Annually each Covered Entity shall submit to the superintendent a written statement covering the prior calendar year. This statement shall be submitted by February 15, certifying that the Covered Entity is in compliance with the requirements set forth. Each Covered Entity shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years. To the extent a Covered Entity has identified areas, systems or processes that require material improvement, updating or redesign, the Covered Entity shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the superintendent.

! The first notice to the superintendent is due February 15, 2018 and annually thereafter.

NATIONAL ASSOCIATION OF INSURANCE COMMISSIONER'S (NAIC) INSURANCE DATA SECURITY MODEL LAW (CYBER MODEL LAW)--OVERVIEW

- Adopted by the full NAIC membership in October of 2017 following over a year and a half of deliberations and numerous drafts

- Purpose and intent of the Cyber Model Law is to establish standards for data security as well as standards for the investigation of and notification to Commissioners of cybersecurity events applicable to all licensees

- Cyber Model Law becomes effective once it is passed by individual states (South Carolina was the first state to adopt the Cyber Model Law)

- Drafting note added to the Cyber Model Law that indicates licensees in compliance with New York's cybersecurity regulations (NYDFS Part 500) are also in compliance with the Cyber Model Law

KEY REQUIREMENTS OF THE CYBER MODEL LAW

	**Breach Notification**	Requirement to notify the Commissioner as promptly as possible, but **no later than 72 hours** following the identification of an event.
	**Information Security Program**	Each Licensee shall develop, implement, and maintain a **comprehensive written Information Security Program** based on the Risk Assessment.
	**ERM Integration**	Licensees shall include **cybersecurity risks in the their Enterprise Risk Management** processes.
	**Incident Response Plan**	Licensees shall establish a **written incident response plan** designed to promptly respond to and recover from cybersecurity events.
	**Risk Assessment**	Licensees shall conduct an **annual risk assessment** of their internal and external threats and, no less than annually, assess the **effectiveness of key controls**, systems, and procedures.

protiviti

California Consumer Privacy Act

What is the California Consumer Privacy Act (CCPA)?

The CCPA is a privacy law that aims to protect consumers' rights by providing them with a greater amount of transparency with respect to how businesses use their personal information. This applies to Californians as well as people whose data is gathered or processed by Californian businesses.

What Can Consumers Do?

The consumer is given the right to:

- Know what information is collected about that consumer.
- Know why that information is collected.
- Request that their information be deleted.
- Request that companies not sell their information.

Who Is Regulated?

Businesses that are for-profit and meet one of these criteria will be regulated by the CCPA;

- Exceed $25 million in gross revenue.
- Participate in the purchase or sale of 50,000 or more consumer records per year for commercial purposes.
- Derive 50% or more of their annual revenue from the sale of personal information.

When Is This In Effect?

When Is This In Effect?

- The CCPA was enacted June 28, 2018 and is effective starting Jan 1, 2020.

Penalties For CCPA Violation

The California Consumer Privacy Act is enforceable by the California Attorney General. The AG can sue for intentional violations up to $7,500 each.

Consumers can sue a business for up to $750 for each violation. Under the CCPA, consumers must give companies a 30 day period to resolve these violations. If the violation is solved and express written notice is made to the consumer, then the consumer cannot issue action for damages.

Source: CCPA

protiviti

CCPA Consumer Rights

Data Rights for Consumers

- Right for a consumer to know all information collected about them by a business.
- Right for a consumer to say no to the sale of their information.
- Right for a consumer to ask that their data be deleted.
- Right for a consumer to be informed of what categories of data will be collected about them prior to its collection.
- Right for a consumer to know the categories of sources of information from whom their data was acquired.
- Mandated opt-in before sale of children's information (under the age of 16).
- Right for a consumer to know the categories of third parties with whom their data is shared.
- Right for a consumer to know the business or commercial purpose of collecting their information.
- Private right of action when companies breach consumer data, to make sure these companies keep that information safe.
- Enforcement by the Attorney General of the State of California.

Other States Creating Data and Privacy Laws

Vermont

Vermont has passed a new law for data brokers that will require them to comply with new rules:

- Better inform consumers on data they collect and how to opt out
- Abide by new security standards.
- Notify authorities of data breaches or failure to meet the security policies.

Colorado

Colorado has passed a new law that will take effect September 1, 2018 for businesses owning, maintaining, or licensing personal information of Colorado residents. As part of this law, these businesses must:

- Maintain a written policy for disposing of personal information.
- Implement appropriate security procedures.
- Comply with breach notification requirements.

Increase in Privacy Awareness

Since Congress cut back on internet privacy regulation this year, the states are now the best chance for strong internet privacy rules. The demand for businesses to comply will keep growing as more states create their own privacy laws in the future.

Contact | **Adam Hamm** | Managing Director | Phone: 312-476-6334 | Email: adam.hamm@protiviti.com

Sources: CAprivacy, Yahoo, Slate

INTERNAL AUDIT'S ROLE & REGULATOR EXPECTATIONS

A. The expectations of regulators will be that companies not only have data controls and processes in place, but that they will also be able to prove that those controls and processes are happening within the environment

B. The Internal Audit Department can help a company prepare for these expectations in a number of ways:

1. Assist in the process of gathering the documentary evidence/artifacts that will be presented to the regulators to establish compliance with data requirements

2. Assist in the process of gathering the evidence/artifacts that will be presented to the regulators to prove that what the company says its doing they're actually doing

3. Assist in the process of educating and preparing the folks in the company that will be meeting with regulators

4. Include in its year to year audit plan pieces of 1-3 above

5. If a company brings in an outside party to do a readiness assessment/mock audit, work with that outside party as they conduct the readiness assessment/mock audit

Face the Future with Confidence

protiviti®