Impact and Preparation for the Surplus Lines Industry

An Overview of the New York Department of Financial Services Cyber Regulations

August 1, 2017
Welcome

Brady R. Kelley
Executive Director
Moderator

Keri Kish
Director of Government Relations
Today’s Panelists

Katherine Armstrong, Drinker Biddle
Larry Hamilton, Mayer Brown
John Connell, United Lex
Marty Schwartzman, SBL Solutions
ELANY Cybersecurity Regulation
Employee Training

- ELANY will bear the expense for training the employees of its active members subject to the terms and conditions noted below (services for up to one year for 417 employees per active member, active members have made an ELANY filing since Jan 1, 2015) as a method to assist members with this particular compliance requirement.

- ELANY has negotiated with Knowbe4 to retain its services on behalf of any active ELANY member which chooses to accept this ELANY funded benefit. ELANY is applying to have this training service meet the New York requirements for CE credits for licensees and sublicensees of active excess line brokers who accept ELANY’s offer.

- Enroll by August 18, 2017

- See Bulletins No. 2017-14, 2017-16, 2017-19)
New York Cyber Regulations

IIABNY Resources for Agents
Visit www.iibany.org/cyber for a dedicated resource page including:

- Compliance chart with deadline dates
- Instructions on how to file for the limited exemption
- Cybersecurity policy template
- Regulation overview webinar recording
- Directory of cybersecurity solution providers
New York Cyber Regulations

27 Days and Counting or Tick Tock

Katherine Armstrong, Drinker Biddle
Larry Hamilton, Mayer Brown
Agenda - Legal Requirements of NY Cybersecurity Regulations

- Framework of Regulations
- Who is covered, exemptions
- Cyber Security Basics
- Compliance and Certification
Regulatory Landscape

- Laws/Regs generally lag behind innovation

- Federal
  - No general federal cybersecurity law
  - Sector specific laws
  - FTC enforcement in data security area
  - Executive orders focusing on cybersecurity
Regulatory Landscape

- State actions
  - 48 State breach notification laws
  - Increasing number of privacy/security laws being introduced by states
  - NY Cyber Regs

- National Association of Insurance Commissioners
  - Model Law (July 2017 Draft)

- Outside of US
  - General Data Protection Act (“GDPR”)
NYDFS Cyber Reg Overview:

- Regulation: 23: NYCRR 500
- Impose minimum standards
- Introduce specific cybersecurity requirements
- Detailed documentation
- Reporting and Certification Obligations
NY Cyber Regs

- Risk Assessment
- Cybersecurity Policies and Procedures
- Cybersecurity Governance & Personnel
- Proactive Cybersecurity Activities
- Cybersecurity Controls
- Cybersecurity Reporting
- Liability for noncompliance

GDPR

- Privacy Impact Assessments and Privacy By Design
- Data Protection Officers
- Recordkeeping; Reporting and Consultation requirements
- Breach Notification
- International Transfers
- Liability and Sanctions for Noncompliance
NY Cyber Regs Requirements

- Requirements
  - Establish a cybersecurity program based on a risk assessment
    - Identify internal and external cyber risks
    - Implement defensive infrastructure and policies and procedures
    - Detect Cybersecurity events
    - Recover from Cybersecurity events
    - Fulfill applicable regulatory reporting obligations
Security Program – based on risk assessment

- **Written Policies**
  - Information security
  - Data governance and classification
  - Asset inventory and device management
  - Access controls and identity management
  - Business continuity and disaster recover planning
  - Systems operations and availability concerns

- Systems network security
- Systems network monitoring
- Systems application development and quality assurance
- Physical security and environmental controls
- Customer data privacy
- Vendor and third party service provider management risk assessment
- Incident response
NY Cyber Regs

- Conduct periodic risk assessments
- Designate a chief information security officer (CISO)
- Employ and train cybersecurity personnel and provide regular cybersecurity aware training to all personnel
- Maintain systems that include an audit trail
- Policies and procedures for secure disposal of nonpublic information
- Implement written third party-information security policies and procedures
- Implement controls to protect information in transit and at rest including:
  - Multi-factor authentication,
    - NY and Model the same
  - Authentication through verification of at least two of the following:
    - Knowledge factors (password), or Possession factors (token, text message), or Inherence factors (biometric)
  - Encryption
  - Limit access privileges
NAIC Insurance Data Security Model Law (July 2017)

- **Implementation of Information Security Program**
  - Develop, implement, and maintain a comprehensive written Information Security Program

- **Objectives**
  - Protect NPI, protect against threats and unauthorized access, periodically reevaluate a schedule for retention of NPI

- **Risk Assessment**
  - Designate an employee, vendor, or affiliate to identify reasonably foreseeable internal or external threats and implement safeguards

- **Risk Management**
  - Design program, based on risk assessment, to mitigate identified risks including
  - Access controls, encryption or other appropriate means, multi factor identification, regular testing and monitoring, audit trails within program, secure disposal, training
NAIC Model Law

- Oversight by Board of Directors
  - Require executive management to write annual reports on Information Security and material matters related to Information Security Program

- Oversight of Third-Party Service Provider Arrangements
  - Written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information held by Third Party Service Providers

- Program Adjustments
  - Monitor, evaluate and adjust as appropriate

- Detailed Incident Response Plan
NAIC Model Law

- Investigation of Cybersecurity Event
- Notification of a Cybersecurity Event
  - Notification to Commissioner
  - Notification to Consumers
  - Notification to Third-Party Service Providers
  - Notification of Reinsurers to Insurers
  - Notice of Insurers to Producers of Record
- Power of Commissioner
- Exceptions
- Enforcement
FTC Data Security Settlement Requirements

- Comprehensive Security Program
- Written procedures, administrative, technical and physical safeguards, appropriate for the size and complexity of the operation
- Designate employee to coordinate and be accountable
- Risk assessments to identify material internal and external risks
  - Consider training, secure engineering, defensive programming, privacy and security by design, review and respond to third party reports, prevent, detect and respond to attacks
- Design and implement reasonable safeguards to control risks identified
- Conduct regular testing or monitoring
- Evacuate and adjust security program based on tests and monitoring
- Best practices for retaining service providers

- 20 year biennial assessments from third party professionals approved by FTC

Assessments must
- Set for specific controls and procedures implemented
- Explain how safeguards are appropriate
- Explain how implemented
- Certify that the program is operating with sufficient effectiveness to provide reasonable assurance that the security of the covered devices or covered information is protected
Writing on the Wall

- Regulatory regimes are fairly consistent
- Compliance with one is NOT compliance with all
- Two kinds of risk
  - Compliance with existing laws and regulations will avoid regulatory sanctions
  - Breach incidents can cause reputational harm and erode consumer trust
Scope of regulation: Covered Entities

• “Covered Entity” is defined as “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” (23 NYCRR 500.19(c))

• Among other things, this includes NYDFS-licensed:
  – insurance companies
  – insurance agents and brokers
  – excess line brokers
  – insurance adjusters

• Whether a licensee is resident or non-resident makes no difference so long as it is NYDFS-licensed
Scope of regulation: Nonpublic Information

• Nonpublic Information is any electronic information that is not publicly available and that is:

  – Business-related information, the unauthorized disclosure or destruction of which would have a material adverse impact on the Covered Entity

  – Information concerning an individual that could be combined with specified data elements to identify the individual, or

  – Derived from an individual or healthcare provider and related to certain healthcare information (except for age and gender)
Entities exempted from Covered Entity status

• By 23 NYCRR 500.19(f):
  – Charitable annuity societies
  – Risk retention groups domiciled outside of New York
  – Accredited and certified reinsurers

• By interpretive letters:
  – Excess and surplus line insurers
Partial exemption for smaller Covered Entities

- Partial exemption is available for Covered Entities that (when aggregated with affiliates) have:
  - fewer than 10 New York employees;
  - less than $5 million in New York revenue; or
  - less than $10 million in total assets.

- Partially exempt Covered Entities must:
  - still comply with: (1) cybersecurity policy and program, (2) access privileges, (3) risk assessment, (4) TSP, (5) data disposal, and (6) NYDFS notice and reporting requirements
  - file a notice of exemption with NYDFS by September 27, 2017 or within 30 days of determining they are exempt (form of notice in Final Regulations, and NYDFS website set-up for filing)
Partial exemption for certain other Covered Entities

- A Covered Entity that does not:
  - have information systems or
  - control or use Nonpublic Information

only needs to satisfy the following requirements:

- risk assessment
- TSPs
- data disposal
- NYDFS notice and reporting

- It must also file a notice of exemption with NYDFS by September 27, 2017 or within 30 days of determining they are exempt
Conditional exemption for employees and agents

- Employees, agents, representatives or designees of a Covered Entity do not need to develop their own cybersecurity program or TSP information security policy IF they are covered by the cybersecurity program or TSP information security policy of the Covered Entity with which they are associated.

- Must file notice of exemption with NYDFS by September 27, 2017 or within 30 days of determining they are exempt.

- Practical tip: If you are going to rely on this exemption, obtain written confirmation from the Covered Entity that you are covered by its cybersecurity program and TSP information security policy.
Third Party Service Providers (TSPs)

- A “Third Party Service Provider” to a Covered Entity is defined as a Person that:
  - is not an Affiliate of the Covered Entity,
  - provides services to the Covered Entity, and
  - maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity.

- If an entity is both a Covered Entity and a TSP, then it is responsible for meeting the requirements of the NYDFS regulation as a Covered Entity.
Implications of being a TSP

- The NYDFS regulation is indirectly applicable to TSPs because Covered Entities must develop written policies and procedures designed to ensure security of systems and data accessible to, or held by, TSPs.

- Covered Entities are expected to perform a risk assessment on their TSPs and conduct due diligence on, and periodic risk-based assessments of, their TSPs’ cybersecurity practices.

- Covered Entities are required to establish minimum term for service contracts with their TSPs addressing:
  - the use of access controls and multi-factor authentication,
  - encryption of Nonpublic Information in transit and at rest,
  - prompt notification to the Covered Entity of certain cybersecurity events, and
  - representations and warranties from the TSPs concerning the policies and procedures that relate to the security of the Covered Entity’s systems or Nonpublic Information.
Potential impact on non-NYDFS-licensed TSPs

• If a non-NYDFS-licensed broker is treated as a TSP by a Covered Entity (e.g., a NY-licensed insurer), then it will be subject to the TSP requirements

• If a non-NYDFS-licensed insurer (such as an excess line insurer) is treated as a TSP by a Covered Entity (e.g., a NY-licensed excess line broker), then it will be subject to the TSP requirements

• All that it takes for a non-affiliate to be a TSP is that it:
  – provides services to the Covered Entity, and
  – maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity
Potential impact on non-NYDFS-licensed affiliates

• When a subsidiary or other affiliate of a Covered Entity presents risks to the Covered Entity’s Information Systems or the Nonpublic Information stored on those Information Systems, those risks must be evaluated and addressed in the Covered Entity’s Risk Assessment, cybersecurity program and cybersecurity policies.

• A Covered Entity is allowed to meet the requirements of the NYDFS regulation by adopting the relevant and applicable provisions of a cybersecurity program maintained by an affiliate. To the extent a Covered Entity relies on an affiliate’s cybersecurity program in whole or in part, that program must be made available for examination by the NYDFS.
Additional practical considerations

• Once an affiliated group of insurance companies has adopted a New York-compliant cybersecurity program for its New York-licensed members that are Covered Entities, there may be practical incentives to implement it for the non-New York-licensed members of the group.

• A parent company may choose to implement its cybersecurity program both for its NYDFS-licensed subsidiaries and for its other subsidiaries, for example, to ensure consistency and efficiency, and to help withstand scrutiny from regulators and the plaintiffs’ bar if a cybersecurity event occurs at one of the members of the group that is not licensed in New York.

• Whether to adopt the NYDFS cybersecurity regulation as an enterprise-wide standard is an issue that many companies are considering as they work through the implementation process.
Cybersecurity Terms

- **Risk assessment – NY defined in 500.09**
  - Establishment of criteria for the evaluation and categorization of identified cybersecurity risks or threats; criteria for the assessment of the confidentiality, integrity, security and availability of the Covered Entity’s Information Systems and NPI; process for dealing with identified risks

- **Risk based authentication**
  - NY – a system of authentication that detects anomalies or changes in use patterns and requires additional verification

- **Chief Information Security Officer (CISO)**
  - NY “a qualified individual responsible for overseeing and implementing the Covered Entity’s cybersecurity program and enforcing its policy.”
Transition periods for compliance

• August 28, 2017 Compliance Deadline: (i) cybersecurity program (500.02), (ii) cybersecurity policy (500.03), (iii) designate a CISO (500.04(a)), (iv) access privileges (500.07), (v) cybersecurity personnel and intelligence (500.10), (vi) incident response plan (500.16), and (vii) notice of cybersecurity event (500.17(a))

• March 1, 2018 Compliance Deadline: (i) CISO reporting (500.04(b)), (ii) penetration testing and vulnerability assessment (500.05), (iv) risk assessment (500.09), (v) multi-factor authentication (500.12) and (vi) enterprise-wide cybersecurity awareness training (500.14(b))

• September 3, 2018 Compliance Deadline: (i) audit trail (500.06), (ii) application security (500.08), (iii) data disposal (500.13), (iv) employee monitoring (500.14(a)) and (v) encryption requirements (500.15)

• March 1, 2019 Compliance Deadline: Third party service provider (TSP) requirements (500.11)
Required notice to NYDFS of cybersecurity events

• Covered Entities are required to notify NYDFS within 72 hours after becoming aware of any cybersecurity event:
  – With a “reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity,” or
  – For which notice must be provided to any government body, self-regulatory agency or other supervisory body

• An attack on a Covered Entity may constitute a reportable cybersecurity event even if the attack is not successful
Annual certification of compliance

- Beginning in 2018, the chairman of the board of directors or a senior officer (i.e., a C-level officer) of the Covered Entity must submit a certification to NYDFS by February 15 of each year
  
  - The certification form is an appendix to the Final Regulation but will need to be completed online
  
  - The form states that to the best of the certifying individual’s knowledge, the Covered Entity’s cybersecurity program complies with the regulation as of the preceding year-end
  
  - If a Covered Entity is not in compliance with all applicable requirements of the regulation, then it is not permitted to submit a certification
Documentation of areas needing improvement

• To the extent a Covered Entity that is in compliance identifies areas that require material updating or improvement, it is required to:
  – Document those areas and the remediation that is underway or planned,
  – Keep the documentation available for inspection by NYDFS, and
  – Retain the documentation for five years
Filing mechanics

• Cybersecurity Notices of Exemption should be filed electronically via the DFS Web Portal
  http://www.dfs.ny.gov/about/cybersecurity

• You will first be prompted to create an account and log in to the DFS Web Portal, then directed to the filing interface

• This account and portal will be used for all regulatory filings relating to cybersecurity, including Notices of Cybersecurity Events and Certifications of Compliance
Closing Remarks
NYDFS Cyber Security Regulations

August 1, 2017
Gap Assessment – What is it?

- A Gap Assessment is an evaluation of whether business requirements are being met – if not, what needs to be done to meet them?
- Capture the current state of your cyber program and determine the areas that require additional efforts to achieve compliance.
- Dependent on your honest input and assessment of what is in place.
  - You may have an information security policy, but is it?:
    - Unfinished?
    - Out of date?
    - Lacking in significant controls?
    - Unseen by many of your employees?
  - Do you really have a policy?
Gap Assessment – What is it?

• Following are the major components of the NYDFS Cyber Regulations:
  – Overall Cyber Program & Policies
  – Chief Information Security Officer & Personnel
  – Penetration Testing & Vulnerability Assessments
  – Auditing
  – Authentication and Access Controls
  – Application Security
  – Risk Assessment
  – Third Party Cyber Risk
  – Data Retention
  – Training
  – Encryption
  – Incident Response Planning
Methodology

• Gather input as a self assessment of your cyber controls. Identify:
  – What is in place
  – What is missing
  – What is partially implemented
• Identify a prioritized set of next steps
• Work towards compliance
UnitedLex’s Approach
UnitedLex’s Approach

2.1 Does your organization maintain the written policies in any of the following areas (check all that apply)?

- Information security
- Data governance and classification
- Asset inventory and device management
- Access controls and identity management
- Business continuity and disaster recovery planning
- Systems operations and availability concerns
- 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

2.3 Were the policies listed above approved by a senior officer of the company or the board of directors?

- Yes
- No
Comments from Marty Schwartzman, SBL Solutions
Questions and Final Remarks from Panelists
Contact Information

Panelists

Katherine Armstrong, Counsel
Drinker Biddle
Katherine.Armstrong@dbr.com

Larry Hamilton, Partner
Mayer Brown
LHamilton@mayerbrown.com

John Connell, Senior Managing Director
United Lex
John.Connell@unitedlex.com

Marty Schwartzman, CPCU
SBL Solutions LLC
MartinSchwartzman@Verizon.net

WSIA

Keri Kish
Director of Government Relations
keri@wsia.org

John Meetz
State Relations Manager
john@wsia.org