CYBERSECURITY
WHAT YOU NEED TO KNOW

iiabny
Independent Insurance Agents & Brokers of New York, Inc.

March 30, 2017
Independent Insurance Agents Assoc of Western NY

What we will cover today

- Broad overview of the regulation
- How did it come about?
- Who does it apply to?
- What do I have to do?
- What is the effective date?
- What is IIABNY doing to assist members with compliance?

How did this come about?

- DFS was developing for over a year
- Initial proposal introduced September 2016
- IIABNY's efforts to improve the proposal
- Revised proposal published December 28, 2016
- Final version published February 16, 2017
- Next steps

Important Definitions

Covered Entity: 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.

Basically any entity regulated by the DFS!

Important Definitions

"Person" is further defined as:

Any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association

Important Definitions

Cybersecurity Event: 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.

Notice to the Superintendent

- Must notify the Superintendent as promptly as possible but no event later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following:
  - *Notice is required to be provided to any government or supervising body or agency*
  - *Has a reasonable likelihood of materially harming any material part of normal operations of the Covered Entity*

Important Definitions

Information System: a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

Important Definitions

Information System: a discrete set of **electronic information resources** organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

Important Definitions

Nonpublic Information: All electronic information that is not Publicly Available Information

Examples: Social Security number, Driver's license, credit or debit card, certain bank account information

Important Definitions

Third Party Service Provider: a person that (i) is not an affiliate of a 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.

Example: Agency management systems

Program vs. Policy

Program – based on risk assessment and covers core *cybersecurity functions*, such as:

- Identify & assess internal and external risks
- Use defensive infrastructure and implement policies & procedures
- Detect, respond to and recover from cyber events
- Fulfill regulatory reporting obligations

Program vs. Policy

Policy – the "how to", based on risk assessment and covers *policies & procedures*, such as:

- Information security
- Data governance, asset inventory, device management
- Access controls
- Network security & monitoring
- Vendor & Third Party Service Provider management
- Incident response

Who is subject to the regulation?

Covered Entities:

- Insurance agencies
- Insurance companies
- Banks and other financial institutions

Limited Exemption

- Fewer than 10 employees (including independent contractors) *of the Covered Entity or its Affiliates located in New York or responsible for business of the Covered Entity* OR
- Less than $5 million in gross annual revenue in each of the last 3 years *from New York business operations of the Covered Entity and its Affiliates* OR
- Less than $10 million in year-end total assets, including assets of all affiliates

Most IIABNY members will qualify for one of these

Other Limited Exemptions

- Employee, agent, representative or designee of a Covered Entity, who is itself a Covered Entity, to the extent covered by the cybersecurity program of the Covered Entity

Other Limited Exemptions

- A Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems and that does not, and is not required to, directly or indirectly, control, own, access, generate, receive or possess Nonpublic Information

Other Limited Exemptions

- A Covered Entity under Article 70 of the Insurance Law that does not and is not required to directly or indirectly control, own, access, generate, receive or possess Nonpublic Information other than information relating to its corporate parent company (or Affiliates)

Other Limited Exemptions

- Persons subject to Insurance Law Section 1110
- Persons subject to Insurance Law 5904
- Any accredited reinsurer or certified reinsurer that has been accredited or certified pursuant to 11 NYCRR 125

Provided that they do not otherwise qualify as a Covered Entity

What are the requirements?

All Covered Entities, including those qualifying for a limited exemption (**must** file a notice of exemption with DFS) must:

- Establish a cybersecurity program and implement cybersecurity policies to protect its Information System
- Limit and periodically review access privileges
- Conduct periodic risk assessment of Information System

Additional Requirements (Limited Exemption)

- Implement policies and procedures to secure information accessible to Third Party Service Providers
- Establish policies for disposal of Nonpublic Information no longer needed
- Provide notice to Superintendent of a Cybersecurity Event
- Annual Certification of Compliance to DFS

Additional Requirements (NOT subject to Limited Exemption

Those who do NOT qualify for the Limited Exemption must also:

- Conduct penetration testing and vulnerability assessments
- Establish an audit trail
- Employ cybersecurity personnel
- Train employees and monitor users
- Use multi-factor authentication

Additional Requirements (NOT subject to Limited Exemption

- Implement controls, including encryption where feasible, to protect data at rest and in transit
- Establish secure development practices for in-house developed applications
- Designate a Chief Information Security Officer (CISO)
- Develop an incident response plan

Compliance Dates

- Effective date **March 1, 2017** with 180 days to comply (**August 28, 2017**)
  - Establish cybersecurity program and policies
  - Limit and periodically review access privileges
  - Provide notice to Superintendent of a cybersecurity event
  - **February 15, 2018** – File 1st annual certificate of compliance with DFS (and every Feb15 thereafter)

Transitional Periods

Transitional periods for certain parts of the regulation:

- **March 1, 2018** (one year) – penetration testing, risk assessment, multi-factor authentication, employee training
- **September 1, 2018** (18 months) – audit trail, app security, data retention, policy to monitor authorized users, data encryption
- **March 1, 2019** (two years) – Third Party Service Providers security policy

Transitional Periods Inconsistency

- Cybersecurity program and policy (based on risk assessment) deadline is **August 28, 2**017 BUT…
- **March 1, 2018** deadline to comply with risk assessment
- We are clarifying with the DFS

What is IIABNY doing for you?

- Continue to work with DFS
- Webinars
- Local Association programs
- Cybersecurity policy template
- Resource list of solution providers
- Dedicated web page
  www.iiabny.org/cyber

Questions?

Support Our Efforts!

- Support IAPAC – your State political action committee
- Bi-partisan support for candidates and legislators in Albany who share our business concerns
- An easy way to support IIABNY's advocacy activities
- www.iiabny.org/iapac

iapac independent agents political action committee
MAKING A DIFFERENCE IN NEW YORK

Contact Information:

Kathy Weinheimer
Senior VP Industry Relations, IIABNY
kweinheimer@iiabny.org
800-851-8853, ext. 239

For more information
www.iiabny.org/cyber

iiabny Independent Insurance Agents & Brokers of New York, Inc.

www.iiabny.org

Proudly Serving Trusted Choice Independent Insurance Agents