Understanding the NAIC Insurance Data Security Law

Dec. 6, 2017

an independent member of
BAKER TILLY
INTERNATIONAL

Baker Tilly refers to Baker Tilly Virchow Krause, LLP,
an independently owned and managed member of Baker Tilly International.

BAKER TILLY

Candor. Insight. Results.

Agenda

BAKER TILLY

Candor. Insight. Results.

01 Cybersecurity trends

02 Insurance Data Security Law overview

03 Comparison to NYSDFS regulation

04 Key takeaways and Q&A

Cybersecurity trends

In the news

BAKER TILLY

Candor. Insight. Results.

CNBC HOME U.S. NEWS MARKETS INVESTING TECH MAKE IT VIDEO SHOWS

TECH TRANSFORMERS | A CNBC SPECIAL REPORT

TECH | MOBILE | SOCIAL MEDIA | ENTERPRISE | CYBERSECURITY | TECH GUIDE

Criminals could use CIA and NSA hacking toolkits for further cyberattacks, experts warn

- The WannaCry ransomware was able to use an exploit in Windows which was originally discovered and used by the National Security Agency (NSA).
- Cybersecurity experts warned that leaks of NSA and CIA hacking tools could lead to more hackers exploiting them.

CNN

WannaCrypt ransomware attack should make us wanna cry

By Alexander Urbelis

Ooops, your files have

What Happened to My Compu

Your important files are encrypted.

Many of your documents, photos, video:

accessible because they have been encry

recover your files, but do not waste you

our decryption service.

will be raised on

Can I Recover My Files?

Top stories

TECH

HACKING OF AMERICA

JAN 30 2017 7:31 AM ET

More Than 4 Billion Data Records Were Stolen Globally in 2016

by HERB WEISBAUM

SHARE

Share

Tweet

Email

Print

Cybercriminals are stealing data at an alarming rate. Both the number of breaches and the number of files stolen globally in these hacks rose dramatically to set a new record in 2016, according to a new report from Risk Based Security. The 4,149 confirmed breaches exposed more than 4.2 billion records. That's approximately 3.2 billion more records than were exposed in 2013, the previous all-time high.

Businesses were the prime targets, with more than half (55 percent) of the reported breaches. But hackers also attacked medical institutions and government agencies.

"The number of records compromised just went completely off the charts," said Inga Goddijn, executive vice president of Risk Based Security. "And as staggering as they are, our numbers probably underestimate the actual criminal activity that's taking place."

Google Docs users hit with sophisticated phishing attack

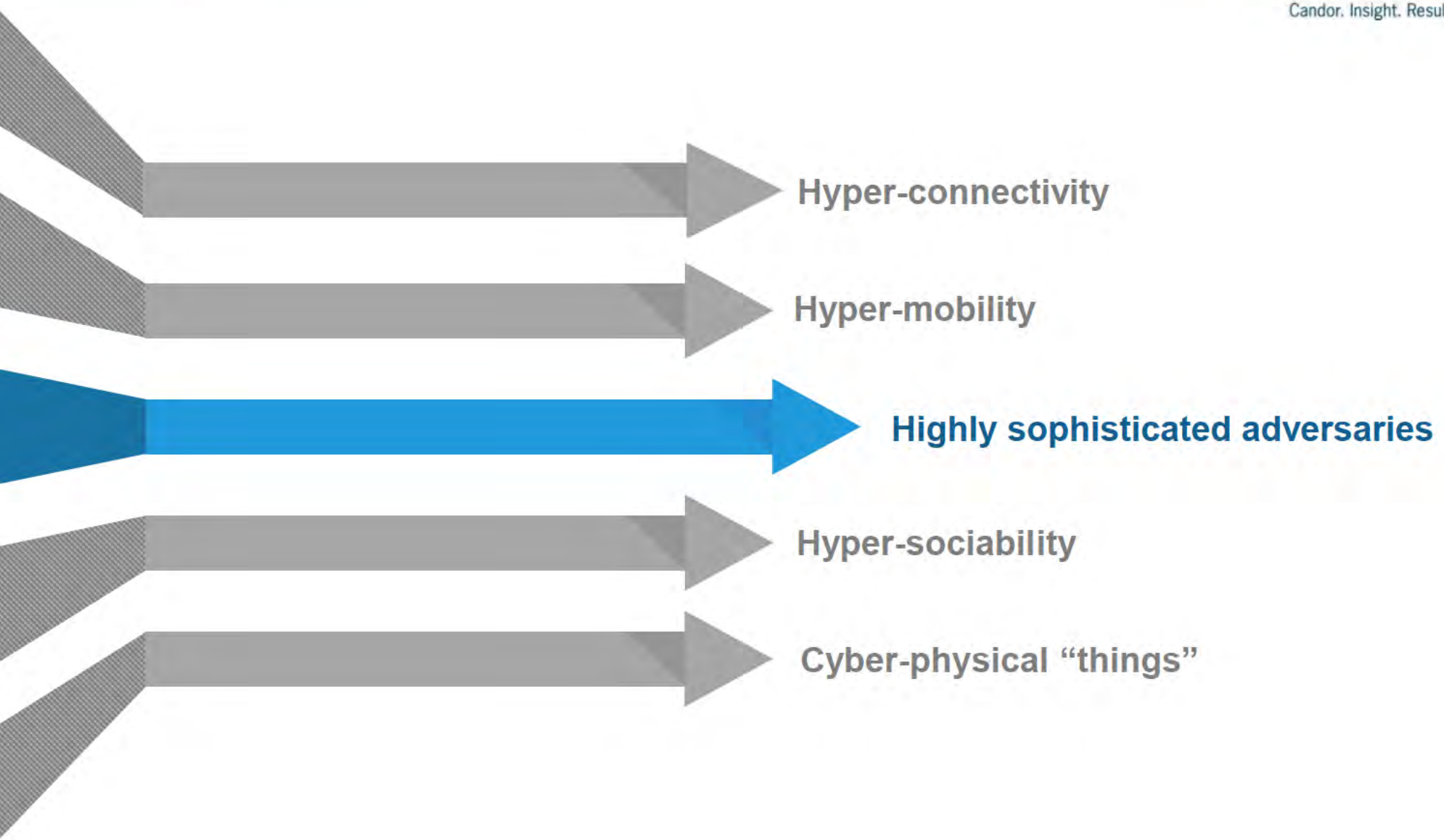
by Adi Robertson | @thedextracity | May 3, 2017, 3:33pm EDT

SHARE TWEET LINKEDIN

Society has become highly digital

BAKER TILLY

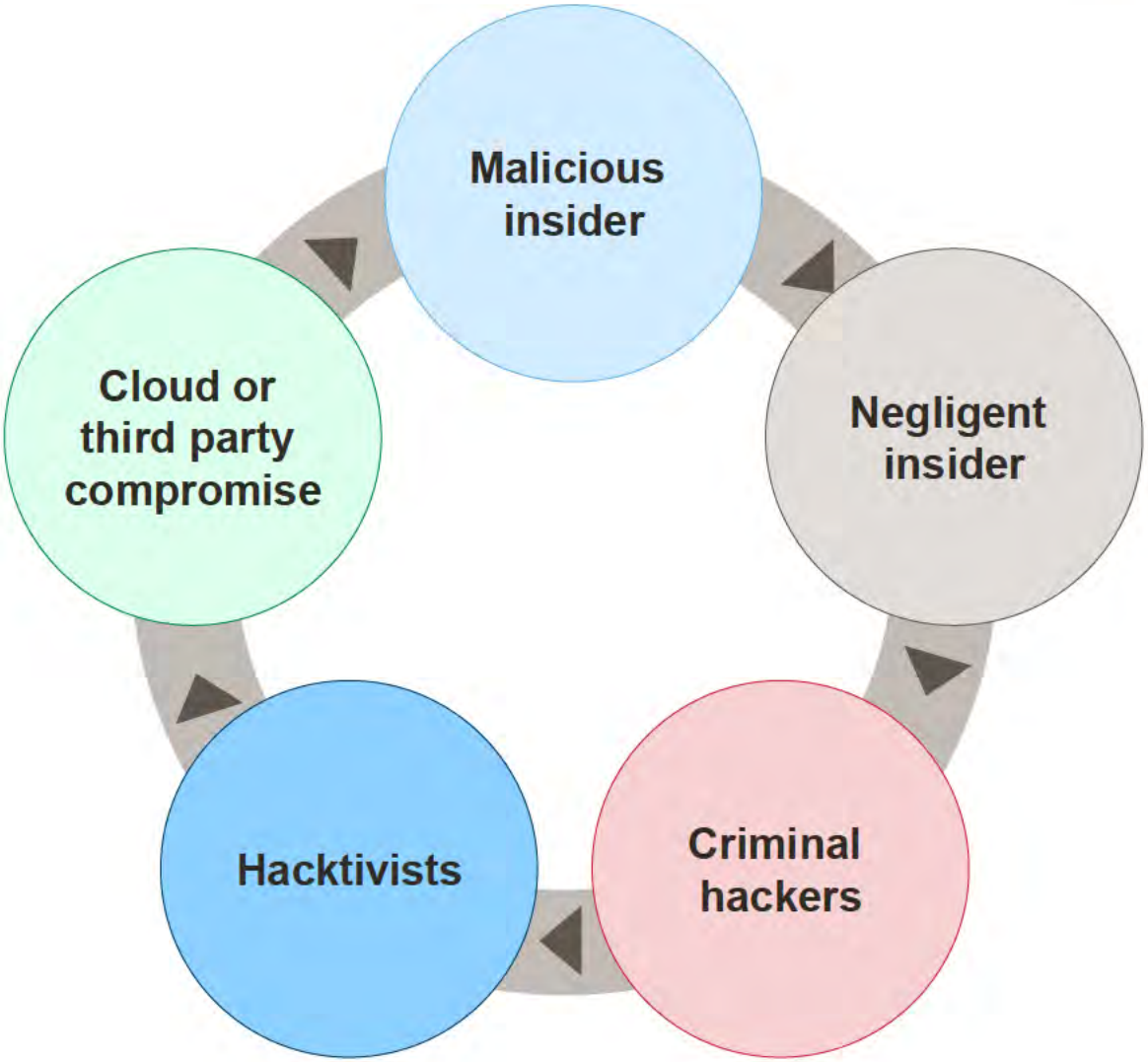
Candor. Insight. Results.



The threat environment

BAKER TILLY

Candor. Insight. Results.



The top threats we face

BAKER TILLY

Candor. Insight. Results.

Socially engineered malware	Password phishing attacks	Unpatched software
Social media threats	Advanced persistent threats	Vendor insecurity

Polling question one

BAKER TILLY

Candor. Insight. Results.

How would you rate your organization's readiness as it relates to the NAIC Insurance Data Security Model Law?

a) We maintain a robust information security program, which meets the requirements.

b) We have a information security program in place that covers most of the requirements and have a plan to address the gaps.

c) We have some of the components addressed, but need to develop a plan to address the gaps.

d) We have few components in place, compliance will require significant effort by our company.

Insurance Data Security Law overview

Insurance Data Security Model law

BAKER TILLY

Candor. Insight. Results.

NAIC
National Association of Insurance Commissioners

NEWS RELEASE

FOR IMMEDIATE RELEASE

NAIC Passes Insurance Data Security Model Law

Cybersecurity model law creates information security standards for insurers

WASHINGTON (Oct. 24, 2017) — The National Association of Insurance Commissioners adopted the Insurance Data Security Model Law today during a joint meeting of the Executive (EX) Committee and Plenary.

The model law, adopted during National Cybersecurity Awareness Month, creates rules for insurers, agents and other licensed entities covering data security, investigation and notification of breach. This includes maintaining an information security program based on ongoing risk assessment, overseeing third-party service providers, investigating data breaches and notifying regulators of a cybersecurity event.

"Considering the recent series of data breaches, cybersecurity is more important now than ever," said Ted Nickel, NAIC President and Wisconsin Insurance Commissioner. "Regulators have a critical role to play in protecting consumers as the cyber landscape continues to evolve and this model law sets cybersecurity customs for insurers to help safeguard consumers."

The model law progressed through the NAIC Innovation and Technology (EX) Task Force and the Cybersecurity (EX) Working Group during the NAIC's Summer 2017 National Meeting. The working group solicited input from regulators as well as industry and consumer representatives throughout the drafting process.

"We've made significant progress on cybersecurity this year and passing this model law creates a platform that enhances our mission of protecting consumers," said Raymond G. Farmer, NAIC Secretary-Treasurer, South Carolina Insurance Director and chair of the Cybersecurity (EX) Working Group.

http://www.naic.org/Releases/2017_docs/naic_passes_data_security_model_law.htm

NAIC – Insurance Data Security Model Law

BAKER TILLY

Candor. Insight. Results.

Section 1. Title
Section 2. Purpose and Intent
Section 3. Definitions
Section 4. Information Security Program
Section 5. Investigation of a Cybersecurity Event
Section 6. Notification of a Cybersecurity Event
Section 7. Power of Commissioner
Section 8. Confidentiality
Section 9. Exceptions
Section 10. Penalties
Section 11. Rules and Regulations
Section 12. Severability
Section 13. Effective Date

NAIC
National Association of Insurance Commissioners

A. Implementation of an **Information Security Program**
B. Objectives of Information Security Program
C. **Risk Assessment**
D. Risk Management
E. Oversight by Board of Directors
F. Oversight of **Third Party** Service Provider Agreements
G. Program Adjustments
H. **Incident Response Plan**
I. **Annual Certification** to Commissioner of Domiciliary State

Source: http://www.naic.org/cmte_ex_cswg.htm

Purpose and intent

BAKER TILLY

Candor. Insight. Results.

The purpose and intent of this act is to establish standards for data security and standards for the investigation of and notification to the commissioner of a cybersecurity event applicable to licensees, as defined in Section 3.

Data security standards

Notification of a cybersecurity event

BAKER TILLY

Candor. Insight. Results.

Cybersecurity event:

> "Cybersecurity event" means an event resulting in unauthorized access to, disruption or misuse of, an information system or information stored on such information system.

> The term "cybersecurity event" does not include the unauthorized acquisition of encrypted nonpublic information if the encryption, process or key is not also acquired, released or used without authorization.

> “Cybersecurity event” does not include an event with regard to which the licensee has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed.

BAKER TILLY

Candor. Insight. Results.

Nonpublic information (NPI):

> "Nonpublic information" means information that is not publicly available information and is:

- Business related information of a licensee the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the licensee.
- Any information concerning a consumer which because of name, number, personal mark, or other identifier can be used to identify such consumer, in combination with any one or more of the following data elements:
  - » Social Security number
  - » Driver's license number or non-driver identification card number
  - » Account number, credit or debit card number
  - » Any security code, access code or password that would permit access to a consumer's financial account
  - » Biometric records

Section 4. (A. B.)
Information security program

BAKER TILLY

Candor. Insight. Results.

> Written information security program:

- Commensurate with the size and complexity of the licensee
- Based on the licensee's risk assessment

> Objectives:

- Protect the security and confidentiality of nonpublic information and the security of the information system
- Protect against any threats or hazards to the security or integrity of nonpublic information and the information system
- Protect against unauthorized access to or use of nonpublic information, and minimize the likelihood of harm to any consumer
- Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction when no longer needed

Section 4. (C.)
Risk assessment

BAKER TILLY

Candor. Insight. Results.

- Identify reasonably foreseeable internal or external threats and assess the likelihood and potential damage.
- Assess the safeguards in place. Considering the following:
  - Employee training and management
  - Information systems, including network and software design, as well as information classification, governance, processing, storage, transmission and disposal
  - Detecting, preventing and responding to attacks, intrusions or other systems failures
- No less than annually, assess the effectiveness of the safeguards' key controls, systems and procedures.

BAKER TILLY

Candor. Insight. Results.

Based on its risk assessment, determine which security measures listed below are appropriate to implement:

- Access controls
- Physical security
- Protect by encryption or other appropriate means, NPI in transit and stored on laptop or other portable storage/media
- Adopt secure development practices and assess third party applications
- Utilize effective controls, which may include multi-factor authentication
- Regularly test systems and procedures
- Include audit trails to reconstruct material financial transactions
- Procedures for the secure disposal of NPI
- Stay informed regarding emerging threats
- Provide personnel with cybersecurity awareness training

Polling question two

BAKER TILLY

Candor. Insight. Results.

The foundation for the information security program is risk assessment and ongoing risk management. Describe your organization's risk assessment and risk management approach?

a) We maintain a mature risk assessment and risk management program which includes ongoing adjustments as risks change.
b) We have a risk assessment and risk management program, but are inconsistent with the execution of the program.
c) We lack a formalized approach to risk assessment and risk management.

BAKER TILLY

Candor. Insight. Results.

Report in writing at least annually:

- The overall status of the information security program and the licensee's compliance with this act
- Material matters related to the information security program, addressing issues such as:

Risk assessment	Risk management and control decisions	Third party service provider arrangements
Results of testing	Cybersecurity events or violations and management 's responses thereto	Recommendations for changes in the information security program

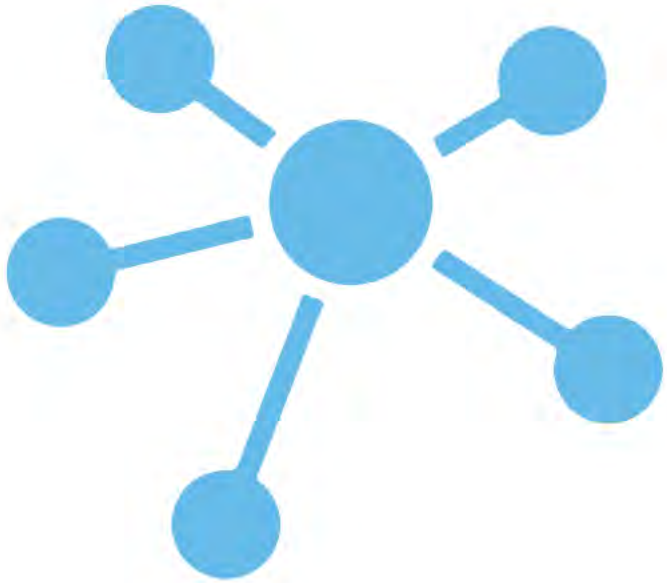
Section 4. (F.)
Oversight of third party providers

BAKER TILLY

Candor. Insight. Results.

"Third party service provider" means a person, not otherwise defined as a licensee, that contracts with a licensee to maintain, process, store or otherwise is permitted access to nonpublic information through its provision of services to the licensee.

- Exercise due diligence in selecting its third party service provider
- Require a third party service provider to implement appropriate administrative, technical and physical measures



Note on effective date: This Act shall take effect on [insert a date]. Licensees shall have one year from the effective date of this Act to implement Section 4 of this Act and two years from the effective date of this Act to implement Section 4F of this Act.

Section 4. (H.)
Incident response plan

BAKER TILLY

Candor. Insight. Results.

As part of its information security program, each licensee shall establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event that … the plan shall address the following:

- The internal process for responding to a cybersecurity event
- The goals of the incident response plan
- The definition of clear roles and responsibilities
- External and internal communications and information sharing;
- Identification of requirements for the remediation
- Documentation and reporting regarding cybersecurity events

Section 4. (I.)
Annual certification

BAKER TILLY

Candor. Insight. Results.

Annually, each insurer domiciled in this State shall submit to the commissioner, a written statement by Feb. 15, certifying that the insurer is in compliance with the requirements set forth in Section 4 of this act. Each insurer shall maintain for examination by the department all records, schedules and data supporting this certificate for a period of five years.

To the extent an insurer has identified areas, systems or processes that require material improvement, updating or redesign, the insurer shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes.

Investigation of a cybersecurity event

BAKER TILLY

Candor. Insight. Results.

If the licensee learns that a cybersecurity event has or may have occurred the licensee or an outside vendor and/or service provider designated to act on behalf of the licensee, shall conduct a prompt investigation.

During the investigation, at minimum:

- (1) Determine whether a cybersecurity event has occurred
- (2) Assess the nature and scope of the cybersecurity event
- (3) Identify any nonpublic information that may have been involved
- (4) Perform or oversee reasonable measures to restore the security

The licensee shall maintain records concerning all cybersecurity events for a period of at least five years from the date of the cybersecurity event .

Section 6
Notification of a cybersecurity event

BAKER TILLY

Candor. Insight. Results.

Each Licensee shall notify the commissioner as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred when either of the following criteria has been met:

- This state is the licensee's state of domicile, in the case of an insurer, or this state is the licensee's home state, in the case of a producer, as those terms are defined in the Producer Licensing Model Act.
- The licensee reasonably believes that the nonpublic information involved is of 250 or more consumers residing in this state and that is either of the following:
  - A cybersecurity event impacting the licensee of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body pursuant to any state or federal law or
  - A cybersecurity event that has a reasonable likelihood of materially harming:
    - Any consumer residing in this state or
    - Any material part of the normal operation(s) of the licensee

Link: Producer Licensing Model Act: http://www.naic.org/store/free/MDL-218.pdf

Polling question three

BAKER TILLY

Candor. Insight. Results.

Which of the following provisions of the NAIC Insurance Data Security Law represents the largest challenge for your organization?

a) Written information security program
b) Risk assessment
c) Board of directors oversight
d) Oversight of third party service providers
e) Incident response plan

Comparison to NYSDFS regulations

Linkage to other rules

BAKER TILLY

Candor. Insight. Results.

Reference to NYSDFS (Page one)

> Drafting note: The drafters of this Act intend that if a Licensee, as defined in Section 3, is in compliance with N.Y. Comp. Codes R. & Regs. tit.23, § 500, Cybersecurity Requirements for Financial Services Companies, effective March 1, 2017, such Licensee is also in compliance with this Act.

Reference to HIPAA (Page 10)

> A licensee subject to Pub.L. 104-191, 110 Stat. 1936, enacted Aug. 21, 1996 (Health Insurance Portability and Accountability Act) that has established and maintains an Information Security Program pursuant to such statutes, rules, regulations, procedures or guidelines established thereunder, will be considered to meet the requirements of Section 4, provided that Licensee is compliant with, and submits a written statement certifying its compliance with, the same.

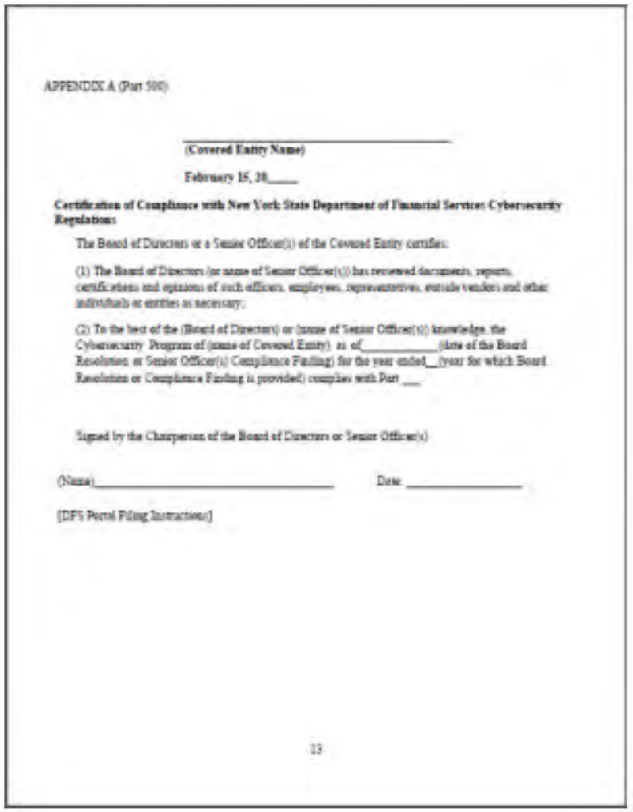
New York State Department of Financial Services (NYSDFS)

BAKER TILLY

Candor. Insight. Results.

[23 NYCRR Part 500 (Financial Services Law)]

Effective March 1, 2017



APPENDIX A (Part 500)

_____
(Covered Entity Name)

February 15, 20____

Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations

The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:

(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;

(2) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity) as of_____(date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended__(year for which Board Resolution or Compliance Finding is provided) complies with Part ___

Signed by the Chairperson of the Board of Directors or Senior Officer(s)

(Name)_____ Date _____

[DFS Portal Filing Instructions]

13

Section	Description
Section 500.01	Definitions
Section 500.02	Cybersecurity Program
Section 500.03	Cybersecurity Policy
Section 500.04	Chief Information Security Officer
Section 500.05	Penetration Testing and Vulnerability Assessments
Section 500.06	Audit Trail
Section 500.07	Access Privileges
Section 500.08	Application Security
Section 500.09	Risk Assessment
Section 500.10	Cybersecurity Personnel and Intelligence
Section 500.11	Third Party Information Security Policy
Section 500.12	Multi-Factor Authentication
Section 500.13	Limitations on Data Retention
Section 500.14	Training and Monitoring
Section 500.15	Encryption of Nonpublic Information
Section 500.16	Incident Response Plan
Section 500.17	Notices to Superintendent

NYSDFS		NAIC	
Section	Description	Section	Description
500.02	Cybersecurity Program	**4**	> Information security program
500.03	Cybersecurity Policy	**4.C.4**	> Assess the sufficiency of policies and procedures
		4.D.2.f	> Modify the information system in accordance with the information security program
500.04	Chief Information Security Officer	**4.C.1**	> Designate an employee, affiliate or vendor who is responsible for the information security program
		4.E.2	> Oversight by board of directors: annual report to the board
500.05	Penetration Testing and Vulnerability Assessments	**4.C.4.c**	> Detecting, preventing and responding to attacks, intrusions and system failures
		4.D.2.h	> Regularly test and monitor systems and procedures to detect actual and attempted attacks or intrusions
500.06	Audit Trail	**4.D.2.i**	> Include audit trails with the information security program designed to detect and respond to cybersecurity events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations
		4.D.2.j	> Implement measures to protect against destruction, loss or damage of nonpublic information
500.07	Access Privileges	**4.D.2.a**	> Place access controls on information systems, including controls to authenticate and permit access only to authorized individuals to protect against the unauthorized acquisition of NPI
		4.D.2.c	> Restrict access at physical locations containing NPI, only to authorized individuals

BAKER TILLY

Candor. Insight. Results.

NYSDFS		NAIC	
Section	Description	Section	Description
500.08	Application Security	**4.D.2.e**	> Adopt secure development practices for in-house developed applications utilized and procedures for evaluating, assessing or testing the security of externally developed applications utilized
500.09	Risk Assessment	**4.C**	> Risk assessment
		4.D.3	> Include cybersecurity risks in the ERM process
		4.G	> Program adjustments
500.10	Cybersecurity Personnel and Intelligence	**4.D.4**	> Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared
500.11	Third Party Information Security Policy	**4.F**	> Oversight of third party service arrangements
500.12	Multi-Factor Authentication	**4.D.2.g**	> Utilize effective controls, which may include multi-factor authentication procedures for any individual accessing nonpublic information
500.13	Limitations on Data Retention	**4.D.2.k**	> Develop, implement and maintain procedures for the secure disposal of NPI in any format
500.14	Training and Monitoring	**4.D.5**	> Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risk identified in the risk assessment
		4.D.2.h	> Regularly test and monitor systems and procedures to detect actual and attempted attacks
500.15	Encryption of Nonpublic Information	**4.D.2.d**	> Protect by encryption or other appropriate means, all nonpublic information while being transmitted over an external network and all nonpublic information stored on a laptop computer or other portable computing or storage device or media
500.16	Incident Response Plan	**4.H**	> Incident response plan
500.17	Notices to Superintendent	**4.I**	> Annual certification to commissioner of domiciliary state

BAKER TILLY

Candor. Insight. Results.

Key takeaways and Q&A

Key takeaways

BAKER TILLY

Candor. Insight. Results.

Understand your systems and data
Identify the data you store, process and transmit. Don't forget about third parties.

Risk assessment
Process not project, should be a living document

Involve others – security is a team sport
All employees and company leaders have a role to play.

Prepare for a cybersecurity event
Assume an event will happen and prepare accordingly.

Disclosure

BAKER TILLY

Candor. Insight. Results.

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

Tax information, if any, contained in this communication was not intended or written to be used by any person for the purpose of avoiding penalties, nor should such information be construed as an opinion upon which any person may rely. The intended recipients of this communication and any attachments are not subject to any limitation on the disclosure of the tax treatment or tax structure of any transaction or matter that is the subject of this communication and any attachments.

Baker Tilly refers to Baker Tilly Virchow Krause, LLP, an independently owned and managed member of Baker Tilly International. © 2017 Baker Tilly Virchow Krause, LLP