Insurance Data Security Model Law

Presented to the

Independent Insurance Agents of Rhode Island

June 13, 2018

Systems Engineering
Get Ahead of IT
syseng.com

What size business are you?

- Small or home office
- Keep files on your PC or Mac
- Use Gmail or get email through 3rd-party
- Use Third-Party SaaS/Cloud LOB apps
- Work as a virtual team
- 10 employees or less

- Small Business
- Have a small network for file storage & sharing.
- Use Exchange / Office 365 for email or get email through 3rd-party
- Use Third-Party SaaS/Cloud LOB apps
- Have management – employee structure
- 10 to 50 employees

- Large Business
- Have complex network for file storage & sharing and LOB applications.
- Use Exchange or Office 365 for email.
- Access to major carrier apps.
- Have a Board of Directors
- 50 Employees and up

Some Quick Definitions

- ISP: Information Security Program
- Nonpublic Information: means information that is not Publicly Available
- Sensitivity: How impactful to your business or the individual is this information.
- PII: Personal Identifiable Information
- PHI: Personal Health Information
- Examples:
  - PII = SSN, Drivers License, Identification Card #, any security code, password or biometric data, account numbers.
  - PHI: Physical and mental health records, healthcare services, healthcare payments

Model Law does not apply to:

- Exceptions to this Act (§9.A)
  - Licensees with fewer than 10 employees.
  - Has a HIPAA Information Security Program in place.
  - A licensed employee or agent.

Section 4.A – ISP Implementation

- What's the scope of your ISP
  - Commensurate with the size and complexity of the Licensee
  - The sensitivity of the Nonpublic Information
  - Covers use of Third-Party Service Providers

Section 4.B – Objectives of ISP

1. Secure and protect systems and PII data they contain.
2. Protect from security hazards, “Threats”.
3. Protect from unauthorized access to and exposure of none public information.
4. Have a record retention policy.

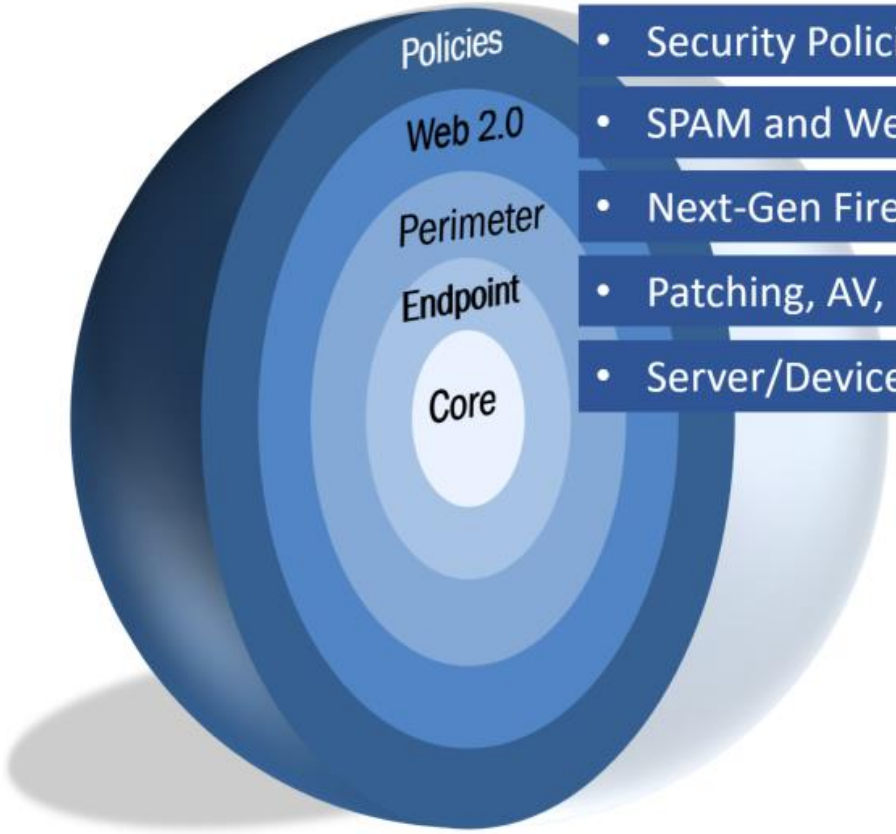
Section 4.C – Risk Assessment

- Identify both internal and external threats to your PII data.
  - This starts with identifying where PII data resides including external third-party service providers.
  - Paper counts as well as electronic data.
- Identify the risk for each of these threats: Risk = Likelihood * Impact
- Assess if your policies, procedures and systems have sufficient safeguards to manage these risks
  - Employee Training
  - Information system governance
  - Threat detection, prevention and response

Section 4.C – Risk Assessment

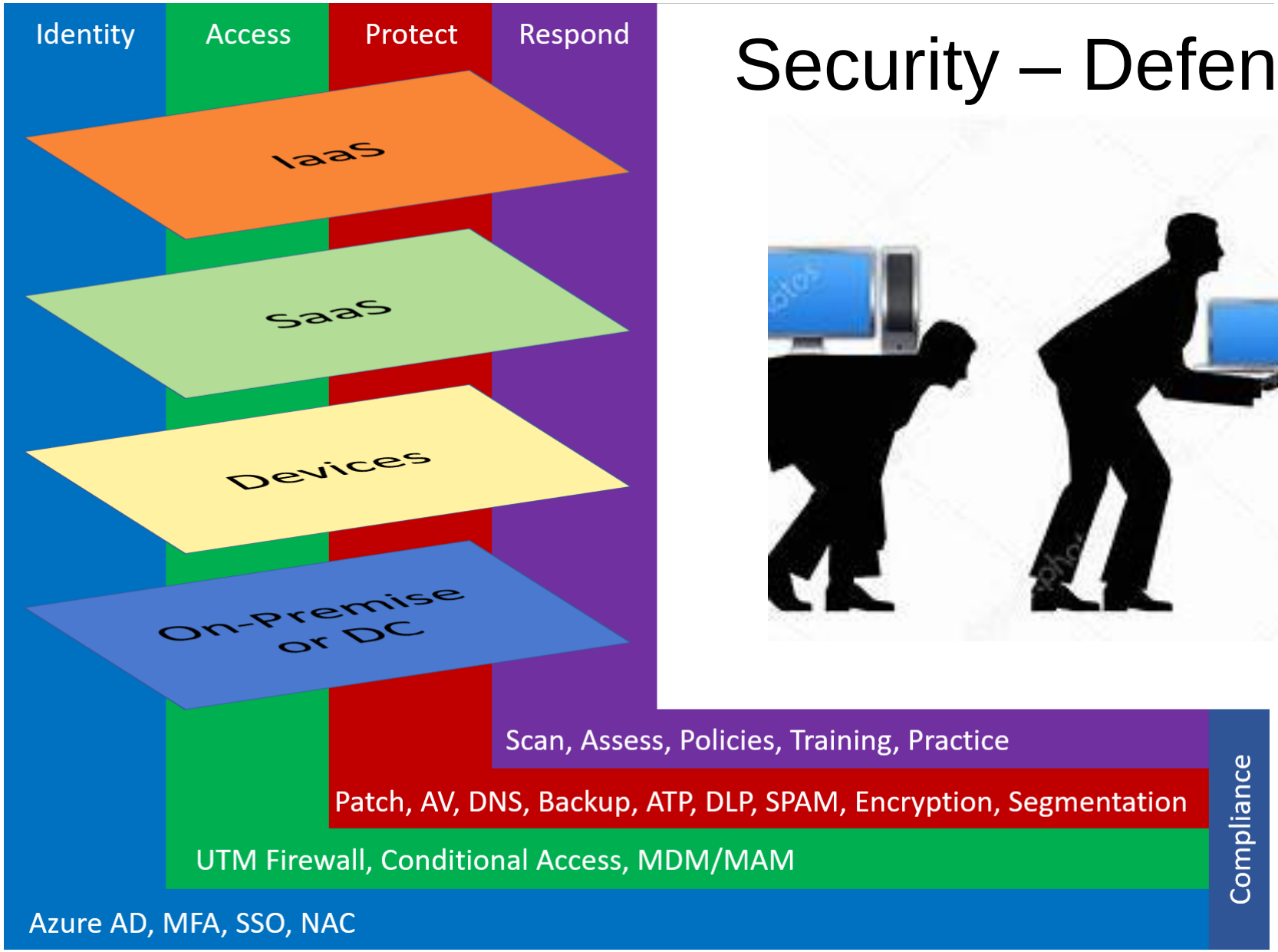
- Potential risks
  - Lost or stolen devices
  - Email
  - Malicious web sites and ads
  - Unpatched computers
  - Wi-Fi
    - Guest Wi-Fi
    - BYOD access to office Wi-Fi
    - Use of public Wi-Fi
  - Human behavior
  - Shadow IT, i.e. Drop Box

Security – Defense in Depth, 2010



- Security Policies, Annual Training
- SPAM and Web Content Filters, 2 Factor Authentication
- Next-Gen Firewall, IPS, AV Gateway, Vulnerability Scan
- Patching, AV, Encryption
- Server/Device Patching, AV, Backup, limit access

Security – Defense in Depth 2018



Section 4.D – Risk Management

Based on the Risk Assessment, design an Information Security Program [ISP] to mitigate identified risk, including third-parties, commensurate to size and sensitivity of information used.

Section 4.D.2.a – Access Controls on Data

Place access controls on Information Systems, including controls to authenticate and permit access only to Authorized Individuals to protect against the unauthorized acquisition of Nonpublic Information

- Can you centrally control access to data and applications?
- Do you have a written password policy?
  - Requires complex password that must be reset at least every 90 days.
- Is the password policy enforced electronically?

Section 4.D.2.b – Policies & Procedures

Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy

- Do you have a written Information Security Policy?
- Do you have a written Acceptable Use policy?
- Do you have a written Business Continuity plan?

Section 4.D.2.c – Physical Access

Restrict access at physical locations containing Nonpublic Information, only to Authorized Individuals

- Are file cabinets locked?
- Are network servers locked in a separate room with limited access?
  - Preferably located in a secure data center or the cloud.
- Do you know who has access to your office?
- Do you have key-card or keys to enter various areas in the office?
- Do you enforce an automatic screen lock?

Section 4.D.2.d – Data Encryption

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

- Do your cloud based applications use https?
- Have you deployed full disk encryption on laptops?
  - This is built into Windows 10
- Do you force mobile devices accessing your data to be encrypted?

Section 4.D.2.e – Secure Application Development

Adopt secure development practices for in-house developed applications utilized by the Licensee and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Licensee;

- This mostly applies to large agencies developing their own applications.
- Maybe you have a great idea for new insurance app.
- This should be part of your due diligence for third-party solutions.

Section 4.D.2.f – Change Management

Modify the Information System in accordance with the Licensee's Information Security Program

- What procedures do you have in place to assure that policies and behaviors defined in your Information Security Program are systematically implemented.

Section 4.D.2.g – Effective Controls

Utilize effective controls, which may include Multi-Factor Authentication procedures for any individual accessing Nonpublic Information

- Mult-Factor Authentication
  - Something you know (user name & password)
  - Something you have (smartphone or token)
- MFA is much easier to own and use now.
- Additional controls can be added based on risk.

Section 4.D.2.h – Test & Monitor

Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, Information Systems

- Periodically scan network for known vulnerabilities.
- Monitor your firewall and network devices for security related events.
- Perform an annual table top exercise.

2017
14,217 - new vulnerabilities cataloged.

Section 4.D.2.i – Event & Transaction Logs

Include audit trails within the Information Security Program designed to (1) detect and respond to Cybersecurity Events and (2) designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Licensee

1. Sophisticated security tools and professionals can capture what's happening second by second.
2. Line of business apps should be able to recover lost transactions.

- #1 requires services from an MSSP like Systems Engineering.
- #2 is a due diligence question for your application vendor.

Section 4.D.2.j – Risk Management

Implement measures to protect against destruction, loss, or damage of Nonpublic Information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures

- How would you recover from a Ransomware attack?
- Do you have a working backup?
- Do you have a Disaster Recovery Plan and have you tested it?

Section 4.D.2.k – Risk Management

Develop, implement, and maintain procedures for the secure disposal of Nonpublic Information in any format.

- Hard drives in your computers and photo-copiers need to be rendered harmless when no longer in your control.
- Paper with sensitive information shredded.
- Understand your Cloud Data lifecycle.

Section 4.D.3-4 – Risk Management

- §4.D.3 Make cybersecurity risks part of your overall risk management process.
- §4.D.4 Stay informed and share information.
- §4.D.5 Provide staff with cyber security awareness training.

“Cyber criminals relied less on automated attacks and exploits, shifting instead to social engineering.”
ProofPoint

Section 4.E – Oversight by Board of Directors

- Require executive management or its delegates to develop, implement and maintain Information Security Program.
- Require executive management or its delegates to report in writing at least annually.

You own this!

Section 4.F – Oversight of Third-Party Service Providers

- You have the same expectation of your third-party service provider as the model law has of you.
- Perform due diligence and keep vendor management records.
- Think HIPAA Business Associate

Section 4.G – Program Adjustment

- You need to review your risks:
  - Changes in your organization
  - The type and amount of sensitive data you have
  - Changing threats
  - Network changes
- Then adjust program, i.e. policies and procedures, accordingly.

Section 4.H – Incident Response Plan

Establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event.

- Responds
  - Engage with legal and insurance representatives
  - Notification to law enforcement, state, affected individuals
  - Mitigate impact
  - Forensic analysis
- Recover
  - Recover data
  - Manage reputational impact
  - Rebuild/replace affected systems

Section 4.I – Annual Certification

- Submit written statement by February 15th
- Maintain records for examination for a period of five years.

Recommendations

- There are things you can do at the Association level
  - Develop a self assessment
  - Policy Templates
- But much must be done at Agency level
  - Risk Assessment
  - Policy development & maintenance
  - Implement appropriate security controls
  - Require annual Security Awareness training
  - Perform a table top exercise to test your policies
- Confider the benefits of going to the “Cloud”

Finding the right Cybersecurity Partner

- Services to look for:
  - Policy Development and management
  - Vulnerability Scanning
  - Security gap assessment & prioritization
  - Can manage and monitor your network
  - Provides advanced security services
    - Such as security event alerting and response
  - Deep cloud experience
- Find a service provider who wants to partner with you

Contact Information

Systems Engineering

Phone - 888.624.6737

Web - syseng.com

Email - info@syseng.com