

Cyber Liability: What Every Network Should Know

John Immordino, CIC, RPLU, CRM, CIPP/US, CPL

Arlington Roe & Co

1-800-878-9891 ext. 8732

Cell: 317.430.7203

jimmordino@arlingtonroe.com



Managing General Agents & Wholesale Insurance Brokers

Outline

- What are the Privacy and Notification Laws?
- What is Private Information?
- Do you have the exposure?
- What will a breach cost you?
- How can you protect your assets?



10%

Of small
businesses

close their doors

25% file for bankruptcy and

37% were knocked offline for a
period of time



- Almost **50%** of small businesses have experienced a cyber attack.
- More than **70%** of attacks target small businesses.
- Kaspersky Lab discovered more than **360K** new malicious files detected every day.
- **76%** of all scanned web sites have vulnerabilities

To Make Matters Worse...

- Only 1 In 50,000 Cyber Thieves Get Caught
- Can't police the problem
- New compliance laws for the business to juggle
- 2000 – 2003 Legislation Began



Laws and Compliance Requirements

- Required to protect private information
- Required to notify individuals of breach
- Offline/Online content
- Federal Laws/State Laws/Regulatory Agencies/Future Laws
 - Privacy Laws
 - HIPAA (Health Insurance Portability & Accountability Act)
 - GLB (Gramm-Leach-Bliley Act)
 - FTC Act (Federal Trade Commission)
 - FCRA (Fair Credit Reporting Act)

Laws and Compliance Requirements

- Consumer Notification Laws
 - HITECH
 - State Notification Laws Required in 50 states
 - States amending current laws
 - The law applies to electronic and paper records.
 - Broad definition of “Personal Information” to include; digital signature, biometric data, fingerprints
 - Notification should be made without unreasonable delay
 - Must notify the SAG and or CRAs
 - Unauthorized access only or also acquisition
 - 2 years of credit monitoring
 - Private right of action – minimum cybersecurity practices

Laws and Compliance Requirements

- Emerging Laws
 - GDPR, CCPA (15 copy cat laws)
 - More control of your information
 - Private right of action
 - Data Security Laws
 - 25 States
 - "reasonable security procedures and practices"
 - Center for Internet Security's Critical Security Controls
 - 20 total
 - NYDFS & NAIC Model Law
 - 8 states and more on the way

Industry Cyber Security

The First - New York Expanded Cyber Law

- The rules, effective March 1, 2017 will cover over 3,000 financial institutions, making [New York the first US state to put cybersecurity regulations into place.](#) Annual certifications start on February 15, 2018.
- This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion.
- Senior management must file an annual certification confirming compliance with these regulations.
- A regulated entity's cybersecurity program must protect the safety and soundness of the institution and protect its customers.

Industry Cyber Security

The First - New York Expanded Cyber Law

- Exempt business only need to comply with 7 of 16 requirements.
 - Exemption: <10 employees located in NY, <\$5M revenue from NY, <\$10M total assets
- 1. A **cybersecurity program** based on the risk assessment of the covered entity;
- 2. A written **cybersecurity policy** approved by each entity's senior officer or board of directors;
- 3. Periodic **risk assessments** to inform design of the cybersecurity program;
- 4. Policies and procedures applicable to **third-party vendors**;
- 5. Proper **notices to the NYSDFS Superintendent** within 72 hours of a "cybersecurity event;"
- 6. Establish policies for disposal on information no longer needed
- 7. Limit and periodic review of access privileges

Industry Cyber Security

The First - New York Expanded Cyber Law

8. A **Chief Information Security Officer** appointed by each entity to implement the cybersecurity program and oversee qualified cybersecurity personnel;
9. Testing of the program's **penetration and vulnerability**;
10. An **audit trail** for all cybersecurity activity;
11. Procedures for ensuring in-house developed **application** security;
12. **Monitoring** of user access;
13. Multi-factor **authentication procedures** for user access and **encryption** of nonpublic information;
14. A written **incident response plan** to respond to any material cybersecurity event; and
15. Regular cybersecurity awareness **training**.

What is Private Information?

Non-Googleable Information

Protected Health Information = 15% of claims

- Broad Definition
- Any part of Medical Record or Payment History
- PHI linked to 18 Identifiers; name, address, phone, fax, email, SSN, unique account numbers, photograph

Private Identifiable Information = 40% of claims

- Non-Googleable
- Non encrypted
- First initial and last name plus
- SSN, Drivers license number or state ID, account number, passwords

Credit Cards/Financial Information = 32% of Claims

What about Email addresses and Zip Codes?

Who Has The Exposure?

- Does your client have information on their employees?
 - Personal client information, corporate information, credit reports, trade secrets, non-disclosure agreements or information in your CCC?
- Storage location is irrelevant – if you collected it, you own it!

What A Breach Can Cost

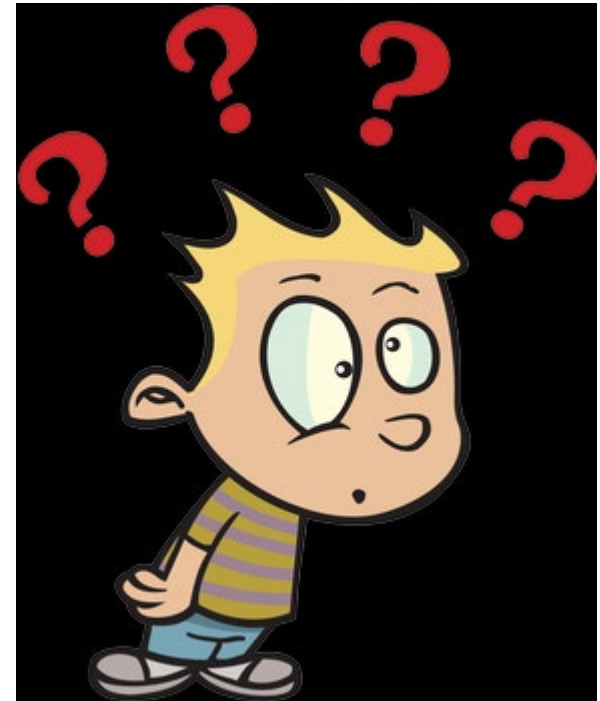
I Have No Idea!

Too Many Variables

**Industry Focuses on
Record Count...**

This Is Flawed

Our Clients Need Something!



What A Breach Can Cost

**Average Cost of a Breach =
\$8,190,000**

- \$242 Per Record (4% increase)
- \$87 = Indirect Costs of abnormal turn caused by adverse publicity – lost business
- \$155 = Direct Costs
 - Detection and Public Relations
 - Notification
 - Ex-post response
- Ponemon Report 2019– actual losses sustained by 64 companies with a 25,575 average record breach

What A Breach Can Cost

Average Cost of a Breach = \$603,700

- 76% - \$459,000 Forensics, legal and notification
- \$50,000 Legal Defense
- \$102,000 Legal Settlement
- \$29,000 Regulatory Defense
- \$ 9,000 Regulatory Fines
- \$25,000 PCI Fines
- Net Diligence – 298 actual insurance claims (2018 report)
 - 1000 median record count (1.2M average)
 - 85% less than \$2B in revenues
 - No consideration for reputation or lost business



*** Caution – this may change*

What A Breach Can Cost

- Reputational Harm
 - #1 Concern of 65% of companies
 - 36% of consumers leave
 - 85% will leave if the breach causes significant person consequences.
 - 49% of breach victims will sue

<http://youtu.be/opRMrEfAiI>

Breach Cost Example

- Community Bank with \$3m Annual Revenues

Category	Risk Response	Cost Factor	Cost per Record
			\$233
Industry Class	Financial	+49%	\$347
Cause of Loss	Negligent Employee	-11%	\$309
Risk Management	Various	-30%	\$216
Revenue Size	Less than \$50M	9170 records	
Breach Size	Less than 10,000 records	100%	\$432

Breach Cost = \$3,961,440

Breach Cost = \$3,961,440

76% Notification = \$3,010,694

24% Liability = \$950,746

Breach Calculators

- <https://databreachcalculator.mybluemix.net/>
- <https://eriskhub.com/mini-dbcc>



It Will Never Happen To Me!

- We have the BEST IT department!
- Sophisticated Criminal Rings
- Firewalls and Virus Protection Software are reactive
- Cause of Data Loss – 2019 Baker Hostetler (3500+ breaches)
 - 34% Phishing (remote access and ransomware)
 - 19% Network Intrusion
 - 17% Inadvertent Disclosure
 - 11% Stolen/Lost Device
 - 6% System Misconfiguration
- Cause of Data Loss – 2019 Beazley (10,000+ breaches)
 - 20% Accidental disclosure
 - 6% Portable devices
 - 8% Social engineering
 - 5% Physical loss of records
 - 47% Hackers or Malware (BEC up 10%)
 - 9% Insider

How to Protect Your Information

- **Focus on the main Causes of Loss**
 - Ponemon, Verizon, Beazley, Symantec, IBM
 - 19% - 53% Negligent Insiders
 - 35% - 49% Hackers/Criminal Attacks
 - 12% - 32% System Glitch
- **Transfer Cost to Insurance – Risk Management In a Can!**

Negligent Insiders

20% of Breaches
were due to unintended disclosure

- Employee Training
 - What is private information and why do they have to protect this online/offline information?

Negligent Insiders

- Be alert to phishing
 - Train employees to identify phishing email



Negligent Insiders

- Email Encryption
 - Microsoft Office 365
 - Implement 3rd party encryption software
 - Ex. RPOST & ZixCorp
 - Scans outbound messages for SSN and encrypts if found
 - Can be easily opened by recipient
 - If recipient has TLS enabled, message is sent transparently
 - \$5-\$15 monthly per user

Negligent Insiders

- Laptop Policy
 - Most of the breaches involving portable devices could've been prevented if the devices were encrypted.
 - Encryption is a safe harbor under virtually every breach notification law.
 - Whole disk encryption
 - *Apple's FileVault*
 - *Window's BitLocker*
 - *Ex. Symantec PGP whole disk encryption*
 - *\$45-\$80 per device*

Negligent Insiders

- Mobile Device Policy
 - PIN required
 - Written policy prohibiting protected information from being stored on a mobile device
- Other Things to Consider:
 - Mobile device security software
 - Ex. Airwatch, Mobile Iron, Maas 360, Good Technologies
 - Allow you to isolate business from personal
 - \$4-\$8 monthly per device

Hackers/Criminal Attacks

- Network Password Policy
 - Breaches due to hacking or malware cost 4.5 times more than the largest loss category. Forensics is expensive!
 - Password reset every 90 days
 - Don't use dictionary words.
 - Add a period to your password or two-factor authentication.
 - $pk9^2chi = 3$ hours to hack, $pk9^2.hi = 24$ hours
 - $pK9^2.hi = 20$ days, $pK9^2.hi. = 5$ years
 - <https://howsecureismypassword.net/>
- Hard to remember so use a phrase
 - !84Ra@tO – 3 days to crack this password
 - ?%iaA>9o – 20 days to crack this password
 - <http://youtu.be/opRMrEfAiI>

Hackers/Criminal Attacks

- Automate patch management
 - 60% of breaches happen to unpatched vulnerabilities
 - 2019, there was a 200% increase in breaches due to malware.
 - Symantec discovered over 246M unique variations of malware in 2018
 - Staying on top of the latest available software patches and automated patch management can protect against a breach.
 - Run in the evening when nobody is using the system
- Virus protection
- Firewalls


Hackers/Criminal Attacks

- Removable Media Security
 - Flash drive
 - Smart phone
 - iPad
 - Tablet
 - External hard drive
- Options
 - Group Policy to disable USB ports, media drives, etc.
 - End Point security software (www.Symantec.com)
 - Encrypt USB drives

System Glitch

- Business process failure
- Application failures
- Inadvertent data dumps
- Logic errors in data transfer
- Authentication failures
- Data recovery failures

*Stuff
Happens
...Insure!*



10%

Of small businesses close their doors and

25% file for bankruptcy

Why Fail?

- They don't know what to do
 1. Must notify promptly or pay the price
 2. Reputational harm is devastating
 3. Cost to comply is expensive
 4. Compliance is a complicated process and involves several professionals.

What Would You Do?

- What would you do if you had a breach?
 - It is a complicated process!
 - Forensics
 - Legal
 - Notification
 - Public Relations
 - Call Center
 - Credit Monitoring
 - Credit Restoration
 - Fined if not reported ASAP.
 - Some states require reporting within 5 days
 - Fines are from \$55k to \$750k for late reporting

What Would You Do?



Networks have unique exposures

- Networks are like snowflakes (all different)
 - Just for profit sharing and commissions
 - Increased market access
 - Operational assistance
 - Perpetuation
 - Marketing assistance
 - Group benefits
 - IT support
 - Risk Management Teams
 - Programs
 - Branding
 - Fee structures and services offered differ....

What Would You Do?

Networks have unique exposures

- Networks are like snowflakes (all different)
 - Because of this, all exposures are different
 - No “One Size Fits All” cyber program
 - Old laws are changing, new ones are emerging
 - Cyber programs need to be broad and unique
 - Master and every member should have cyber insurance
 - Cyber cover is always changing along with appetites
 - Getting all coverage in one policy is a challenge



What Would You Do?



Networks have unique exposures

- Carrier contracts (all different)
 - Cybersecurity compliance requirements
 - RM web portal (cybersecurity program, policy, assessments)
 - Notification within 72 hours
 - Trigger for noncompliance of minimum cybersecurity requirements
 - Responsible for sub-producers
 - IC as insured
 - Trigger for breach of information in CCC and other systems
 - Requirement of third party cybersecurity compliance
 - RM portal for 3rd party policy, risk assessment and provider tracking

What Would You Do?

Networks have unique exposures

- Carrier contracts (all different)
 - Who owns the data?
 - Some carriers say they do, some you do and some are silent
 - Sub creates application, master pulls MVR and carrier pulls credit report. You all own the information.
 - Trigger for breach of information in CCC and other systems
 - No contractual liability exclusion
 - Carriers require indemnification of breach costs
 - WISP, assessments, notification within 24 hrs, encryption and master is required to confirm subs are compliant
 - Coverage for liability assumed under contract
 - No contractual liability exclusion
 - Turnkey incident response but will probably not address the notice to carriers, only regulators.



Industry Cyber Security

The First - New York Expanded Cyber Law

- Exempt business only need to comply with 5 of 13 requirements.
 - Exemption: <10 employees located in NY, <\$5M revenue from NY, <\$10M total assets
- 1. A **cybersecurity program** based on the risk assessment of the covered entity;
- 2. A written **cybersecurity policy** approved by each entity's senior officer or board of directors;
- 3. Periodic **risk assessments** to inform design of the cybersecurity program;
- 4. Policies and procedures applicable to **third-party vendors**;
- 5. Proper **notices to the NYSDFS Superintendent** within 72 hours of a "cybersecurity event;"

What Would You Do?

Networks have unique exposures

- Agency management systems

- Do all members use the same system?
 - Aggregation of data issue depending on size
 - 1st named and named insured with one aggregate and umbrella
- Does the master rent the use of the system?
 - Technology E&O for master
- Do all members have their own?
 - Separate policies with master as AI.
- What happens if the system goes down?
 - Tech E&O, business interruption and dependent BI

- Vicarious Liability

- What name does the sub operate under?
 - Master as additional insured

What Would You Do?

Other Coverages

- Notification on a record count
- Reputational harm
- Invoice manipulation
- Extortion for eCard demands
- Social engineering
- Cryptojacking

John Immordino, CIC, RPLU, CRM, CIPP/US, CPL

Arlington Roe & Co

1-800-878-9891 ext. 8732

Cell: 317.430.7203

jimmordino@arlingtonroe.com

Sources: NetDiligence 2018

Ponemon Institute 2019

PricewaterhouseCoopers Survey

Verizon 2015 DBIR