CHICAGOLAND RISK FORUM
THE CHICAGO RIMS CHAPTER

ChicagoLand RIMS

Cyber Insurance Coverage Pitfalls and How to Avoid Them

PROVIDED BY HUB INTERNATIONAL
October 25th , 2016

AGENDA

1. The evolution of cyber risk & cyber risk insurance policies
2. Costs of a data breach response
3. Key cyber insurance terms, conditions and exclusions.
4. Lessons learned from recent cyber insurance coverage disputes.
5. Strategies to maximize cyber insurance coverage and ways to avoid common pitfalls.

THE EVOLUTION OF “CYBER RISK”

Increased Regulation of Privacy Matters

2006 – FTC levies first privacy fine: $10M against Choicepoint

2008 – First HIPPA corrective action: $100K Providence HC

2011 - First HIPPA fine: $4.3M against Cignet

http://www.hubinternational.com/crisis-management/cyber-risk

THE EVOLUTION OF CYBER INSURANCE

Late 90's - Technology E & O policies - coverage for network failures

Mid 2000's – Coverage for:

- Costs related to accidental disclosure of sensitive data
- Paper records
- Third party lawsuits
- Regulatory investigations

Today – Coverage for:

- Bodily injury & property damage (rare, but possible)
- Dependent business interruption
- Higher limits

PONEMON 2016 CLAIM STUDY

383 companies in 12 countries

$4 million is the average total cost of data breach

15% increase in total cost of data breach since 2013

$158 average cost per lost or stolen record

29% percent increase in per capita cost since 2013

TOP THREATS TODAY

Ransomware

- 2015 - FBI reports 2,453 ransomware incidents, victims paying **$25 million**
- 2016 – **$209 million** paid to through March.*

Phishing Emails / Business Email Compromise

- 23% of recipients open phishing emails and 11% click on attachments**
- 8,200 victims $1.2 billion in actual/attempted losses ***

* *Source: http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/*

** *Source: Verizon 20165 Data Breach Investigations Report*

*** *Source: https://threatpost.com/fbi-social-engineering-hacks-lead-to-millions-lost-to-wire-fraud/114453/*

LEGAL LANDSCAPE

Duties To Protect Data, Imposed By…

- State laws
- Federal laws/regulations
  - HIPAA, GLB/Red Flags, FERPA, etc.
- PCI
- International Laws

ANATOMY OF A BREACH RESPONSE

Internal Client Issues
Internal reporting
Broker involvement
Insurance & Deductible Management

Experts
Breach coach
Forensics
Credit Monitoring
Notification Firms / Call Centers
Public relations

Investigation - internal/forensic/criminal
How did it happen
When did it happen
Is it still happening
Who did it happen to
What was accessed/acquired (**What wasn't**)
Encrypted/protected

Notice Methods
- Written
- Electronic
- Substitute
- Media

Deadlines
- Can be from 15 days to "without unreasonable delay"

Inquiries
- State regulators (i.e. AG)
- Federal regulators (i.e. OCR)
- Federal agencies (i.e. SEC, FTC)
- Consumer reporting agencies
- Plaintiffs

STATE REGULATORY EXPOSURES

State level breach notice: 47 states (plus Puerto Rico, Wash. D.C., Virgin Islands) require notice to customers after unauthorized access to PII/PHI.

- Require firms that conduct business in state to **notify resident consumers** of security breaches of unencrypted computerized personal information
- Many require **notification of state attorney general**, state consumer protection agencies, and credit monitoring agencies
- Notice due “without unreasonable delay”

STATE NOTIFICATION TRENDS

- Email, Passwords, Biometrics = PII
- Less time to notify
- Fines for non-compliance – up to **$200 per record**
- Credit monitoring required
- Notice to attorney general in addition to individuals
- Written information security plan & encryption required
- July 7, 2015 - 47 State AGs write to Congress, urging U.S. to preserve state authority over data breaches

COMMON CAUSES OF ACTION

Plaintiff Demands

- Fraud reimbursement
- Credit card replacement
- Credit monitoring/ repair/ insurance
- Civil fines/ penalties
- Statutory damages
- Time
- Unjust enrichment
- Fear of ID Theft
- Actual ID Theft
- Mitigation costs
- Time spent monitoring

CYBER INSURANCE CONSIDERATIONS

Where

- Online
- Offline

Who

- Malicious
- Accidental
- Internal
- External

What

- Technology
- Media
- Protected Data
  Confidential Information

Financial Impact

- Event Management Expense
- Extra Expense
- Lost Business Income
- Defense Expense
- Regulatory Fine or Penalty and/or Damages

LEGACY INSURANCE COVERAGES

Property Insurance

Malware and Denial-of-Service are not considered "named perils"

Malpractice/E&O

- Requires negligence in professional services
- Generally do not cover regulatory actions

Common Hurdles

Insured vs. Insured Issues

No coverage for Event Management or Reputational Harm

General Liability Insurance

- Intended to cover bodily injury and property damage
- CGL privacy coverage is limited to defamation and slander
- ISO forms have explicitly excluded Cyber coverage after Sony v. Zurich

Crime Coverage

- Crime policies require intent
- Theft of money, securities or tangible property

Cyber Risk

Traditional Policies vs. Cyber Risk Policy

	Property	General Liability	Crime	K&R	E&O	Cyber Risk
1st Party Privacy/Network Risks						
Physical damage to data only		X			X	✓
Virus/Hacker damage to data only		X	X	X	X	✓
DOS (Denial of Service) Attack		X	X	X	X	✓
BI Loss from security event		X	X	X	X	✓
Extortion or Threat	X	X	X	✓	X	✓
Employee Sabotage of data only	X	X		X		✓
3rd Party Privacy/Network Risks						
Theft/Disclosure of private information	X		X	X		✓
Confidential Corporate information breach	X		X	X		✓
Technology E&O	X	X	X	X	✓	**Combinable**
Media Liability (electronic content)	X		X	X		✓
Privacy Breach expense/notification	X	X	X	X	X	✓
Damage to 3rd Party's data only	X			X		✓
Regulatory Privacy Defense/Fines	X	X	X	X	X	✓
Virus/Malicious code transmission	X		X	X		✓

X	Coverage Not Likely		Possible Coverage	✓	Coverage Available

DATA BREACH:
RISK TRANSFER TO INSURANCE

- **Network Security Liability:** liability to a third party as a result of a failure of your network security to protect against destruction, deletion, or corruption of a third party's electronic data, denial of service attacks against internet sites or computers; or transmission of viruses to third party computers and systems.

- **Privacy Liability:** liability to a third party as a result of the disclosure of confidential information collected or handled by you or under your care, custody or control. Includes coverage for your vicarious liability where a vendor loses information you had entrusted to them in the normal course of your business.

- **Electronic Media Content Liability:** Coverage for personal injury, and trademark and copyright claims arising out of creation and dissemination of electronic content.

- **Regulatory Defense and Penalties:** Coverage for costs associated with response to a regulatory proceeding resulting from an alleged violation of privacy law causing a security breach.

DATA BREACH:
RISK TRANSFER TO INSURANCE

- **Breach Event Expenses:** expenses to comply with privacy regulations, such as notification and credit monitoring services for affected customers. This also includes expenses incurred in retaining a crisis management firm, outside counsel and forensic investigator.

- **Cyber Extortion:** payments made to cybercriminals to decrypt data that has been encrypted by ransomware.

- **Network Business Interruption:** reimbursement of your loss of income and / or extra expense resulting from an interruption or suspension of computer systems due to a failure of network security or system failure. Includes sub-limited coverage for dependent business interruption.

- **Data Asset Protection:** recovery of costs and expenses you incur to restore, recreate, or recollect your data and other intangible assets (i.e., software applications) that are corrupted or destroyed by a computer attack.

CYBER INSURANCE COVERAGE

Cyber Insurance Policy Considerations:

- Self Insured Retentions
- Sub-limits
- Do defense costs erode policy limits / SIR?
- Retroactive dates & prior claims

POSSIBLE EXCLUSIONS

- Bodily injury & property damage
- Contractual Liability
- Failure to encrypt
- Acts of Foreign Governments
- Violations of consumer protection laws
- Failure to follow “minimum required practices”
- Losses caused by:
  - “Mechanical failure”
  - “Error in design”
  - “Gradual deterioration of computer systems”

INSURANCE COVERAGE DISPUTES

Ameriforge Group, Inc. v. Federal Insurance Co., et al.,
No. 16cv377 (S.D. Tex.)

- $480,000 loss due CEO impersonation
- Federal denied coverage based on:
  - Coverage limited to **forgeries of actual financial instruments** and not fraudulently signed emails directing the transfer of funds;
  - Coverage **requires a hacking event** whereby unauthorized access to the computer system occurs, not merely a phishing attack through an email
  - No coverage for **voluntary transfers**

Source: https://jenner.com/system/assets/updates/1420/original/ILU_April_2016.pdf?14604496

INSURANCE COVERAGE DISPUTES

BitPay, Inc. v. Massachusetts Bay Insurance Co., No. 1:15cv03238 (N.D. Ga.)

- CEO impersonation, tricked a BitPay client to send $1.85 million to the criminal.
- Massachusetts Bay denied coverage:
  - Coverage only applies to transfer of property from **inside the premises** to a person or place **outside the premises**.
  - Massachusetts Bay also draws a distinction between **fraudulently causing a transfer**, which it says the policy covers, and **causing a fraudulent transfer**, which it says happened here and is not covered.

Source: https://jenner.com/system/assets/updates/1420/original/ILU_April_2016.pdf?14604496

YOUR VENDOR'S CYBER INSURANCE COVERAGE

Insurance requirements – review terms and limits

- Certificates of Insurance
- Are you listed as additional insured?
- "Other Insurance" provisions?
- Coverage territory – worldwide?
- Retro Date – potential claims before retro date?
- Sub-limits for crisis management costs?
- Deductible / SIR : Who can satisfy it? You or vendor?

CYBER INSURANCE COVERAGE

The Claims Process

- Duties to report to insurance carrier
- Multiple policies may apply
- Vendor panels
- Consent to settle
- Subrogation – vendors & contracts

PREVENTING THE DATA BREACH : NETWORK ASSESSMENTS

WHAT THEY DO & HOW THEY HELP:

- Identify, Locate & Classify information assets.
- Conduct threat modeling exercises / penetration testing.
- Evaluate vulnerabilities in people, processes & technology.
- Make recommendations to secure data.
- Benchmark against HIPAA rules, PCI standards & others.

NETWORK ASSESSMENTS

Assessments **could be mandated** by:

- Business partners
- Industry regulators
- Cyber insurance companies

INSURANCE & PRE-BREACH SERVICES

- Cybersecurity Risk Assessments
- “Dark Net” mining & monitoring
- Vendor security ratings
- “Shunning” of known malicious IP addresses
- Mobile Apps – news and claims data
- Online employee education and training

Questions?

John Farley

HUB International
Vice President
Cyber Risk Services

Tel: 212-338-2150
Cell: 917-520-3257
john.farley@hubinternational.com

Emily Selck

HUB International

Vice President & Practice Leader
Cyber Liability

Tel: 312-279-4941

Cell: 312-718-7311

emily.selck@hubinternational.com