How to Sell Cyber Insurance to Different Industries
MODERATOR:
Mickey Estey, Senior Vice President, RT Specialty

PANELISTS:
Manny Cho, Vice President, Regional Underwriting Manager, AXIS Pro
Michael Lamprecht, President, Big Data Insure, LLC
Garin Pace, Head of Underwriting Excellence – Cyber, AIG
Michael Palotay, Senior Vice President, NAS Insurance
1. Epsilon - $100 million-$4 billion
2. Veterans Administration - up to $500 million
3. Hannaford Bros - $252 million
4. Target - $250 million to date
5. Sony PlayStation - $171 million
6. TJ Maxx - $162 million
7. Heartland Payment Systems - $140 million
8. Anthem - $100 million+ to date
9. Sony Pictures Entertainment - $100 million to date
10. The Home Depot - $56 million to date

Source: ALM Media - LifeHealthPro
Breaches directly affecting C-Suite

- OPM Director Resigns After Devastating Hacks
- Target’s Chief Information Officer Resigns
- Target CEO resigns as fallout from data breach continues
- Sony data breach claims first scalp as co-chair steps down
- Texas Comptroller fires several information security execs
- Ashley Madison CEO resigns in wake of hack
- Utah CTO takes fall for data breach
Key steps in the cyber placement process

- **Data collection & exposure assessment** - Amounts and types of data, network/system structure, potential attack vectors or loss scenarios

- **Discuss Costs/Expenses/Losses** - Breach response costs, compliance with legal/regulatory, legal liability depending on industry

- **Data & systems controls/protections presented** - Application, underwriter question answering, underwriting meeting conf/call

- **Evaluate quote options and limits** - Coverage priority, breach response options & vendors, benchmarking, breach costs/expenses modeling

  • **TELL THE TEAM YOU BOUGHT A POLICY!**
Retail
Selling Cyber to Retailers – Current Environment

- There has been a huge explosion in retail data breach frequency over the last 2-3 years.

- Typically caused by malware targeting the merchant’s POS (Point of Sale) machines. (BlackPOS) Retailers are scrambling to upgrade their security systems (and cyber insurance program) to address this threat.

- The Target breach has cost $250M in 2013-2014 ($90M of which was insured) (According to Target’s 8K filing). This number is expected to continue to increase as litigation runs its course throughout 2015. This figure doesn’t include the reduced revenue that Target experienced during the months following the breach.
Underwriting Considerations – What to Expect

Underwriting has tightened considerably for POS exposed insureds in the past 2-3 years. As retailers are looking to increase their limits, insurers are cutting capacity. This has led to a mini hard market.

• **Credit Card Transaction Volume** – Directly proportional to an insurer's expected loss. The large retailers have enormous potential exposure.

• **POS Security Controls** – Tokenization, E2E Encryption (holy grail), Intrusion Detection, Data Leak Prevention.

• **Still running Windows XP? PCI Compliant?**
Trends that you need to be aware of

• **Chip and Pin Liability Shift** – October 1st. What does this mean for your insureds? How does it impact their cyber policy? (hint – not much)

• **Neiman Marcus Decision** - Breached customers have standing now, can’t rely upon Clapper for protection.

• **Larger Limit Towers** - Target breach illustrated to many retailers that they were not sufficiently insured.

• **Lost revenue as a result of a damaged reputation following a breach** – Target experienced a significant dip in overall transaction volume, and revenue in the weeks/months, following their data breach.
PCI Coverage - What you need to know

If a Merchant is Breached, they may be responsible to pay the following:

• PCI Fines/Penalties due to non compliance (Cost varies between the various card associations).

• All or a portion of the fraud losses associated with the compromise (from the date of the compromise forward) – (can be as high as $25 - $50 per card).

• Any additional fraud prevention/detection costs incurred by credit card issuers associated with the compromise (i.e. additional monitoring of system for fraudulent activity).

• It is crucial to make sure that all the above is covered by the cyber policy.
Common Objections

• We don’t store the credit card information.
• We outsource the payments to a POS vendor.
Healthcare
Healthcare Exposures

- **Various Sizes**
  - Small / Medium / Large
- **Various Shapes**
  - Doctors/Dentists
  - Physician Groups
  - Hospitals / Hospital Groups
  - Medical Billing / TPA’s
  - Insurance Carriers
  - Allied Medical
  - Specialty Areas
- **Every Business Carries PHI**
Healthcare Exposures

• **Spam Nation**
  – White Listed Servers
  – Take Over vs Breach

• **Exposed to the Four “P”’s**
  – PII / PHI / PCI / Paper
    • Where is the Data?
    • How is it protected
  – PHI Value vs Cost of Notification

• **EHR / EMR**

• **Mobile Applications**

• **Business Associates**
  – Compliance / Tracking

• **State Laws (CMIA)/ Canada**
HIPAA the Solution

• Unfortunately Not the Total Solution...

• As of 8/4/2015*
  – 446 Breaches (783 in 2014)
  – 139M Records Exposed
  – 78.8M Anthem / 21.5M US Office Personnel Mgmt

• Recent HIPAA Fines**
  – $218,400 - St. Elizabeth’s Medical Center – Use of cloud based document sharing service / lack of risk assessment and mitigation – 498 records stored on ePHI
  – $750,000 – Cancer Care Group – breach in 2012, but before that time out of compliance – lacking policies and controls – 55,000 records on laptop

• $28.2M in Settlement involving 28 organizations**
  – Largest - $4.8M – NY Presbyterian Hospital and Columbia University Medical Center*
  – Average Settlement is $1.1M*

*source IDTheft Resource Center ** Health and Human Services
Healthcare Largest Exposure

• People Can Defeat the Best Security Practices
• Healthcare Breaches 2015*
  – 32% caused by crime
  – 31% caused by lost / stolen device
  – 29% caused by employee error
  – 8% caused by malicious insider

*hipaajournal.com
UW Evaluation

• HIPAA Compliance – Baseline
• Data = Quantifying the Risk
  – How Much?
    • Current / Historical / Purging
  – Review / Mapping / Tracking
  – Segmentation
  – Authorization / Authentication
  – Encryption
    • Hardware / Laptops / Mobile
    • CMIA Impact
  – Managing Business Associates
    • EMR / EHR Agreements
    • Compliance Tracking / Enforcement
UW Evaluation

• **Social Engineering**
  – Awareness / Phishing Exercise

• **Incident Response**
  – Plan / Process / C-Suite Involvement

• **PCI Compliance**
Selling Cyber Risk Coverage to Professional Services Firms
Identifying Industry Based Exposures

3rd Party Liability
- Privacy Breaches
- Confidentiality Breaches
- Regulatory Violations
- Theft of client funds
- Loss of client data
- Professional rule violations
- Denial of access
- Defamation
- I.P. Infringement

1st Party Property
- Data Damage/Loss
- System degradation/Interruption
- Interruption of access
- Theft of money or other property
- Reputational Injury

Confidentiality and Privacy
Data/Network Integrity and Availability
Cyber/E&O
Money, Securities and other Property
Advertising and Publishing

September 17th, 2015 • Chicago, IL
Cyber Risk Insurance Marketplace

Stand Alone Market
• 18 markets with dedicated forms for professionals
• Typical Limits of $10-$25mm
• Broad Coverage includes
  – Media Liability
  – Network Security & Privacy
  – Data Restoration
  – BI/EE
  – Extortion / Crime
  – Brand Protection

Endorsement/Embedded in E&O Policy
• Over 20 markets with “free” cyber risk coverage extensions.
  – Limits range from 10k – 250k
  – Varied & Limited coverage
  – Frequently designed to protect E&O limits
    *There is no such thing as “free” cyber coverage*

• 5 Markets that sell embedded coverage
  – Blended or stand alone limit
  – Good quality coverage
  – Biggest advantage: does not have a 2nd set of T&C

• Over 10 markets that sell add on coverage comparable with stand alone

75% of all professional firms will have cyber coverage by end of 2016
What to Look For

• Robust Industry Specific Breach Response Packages
• Definition of Insured
• Professional Services Exclusions
• Net Profit Before Tax BI/Models
• Other Insurance Clauses
• Encryption/Security Warranties
• Contractual Risk Transfer Requirements
• Crime/Extortion triggers
• LPL/GL/EPL/Property/Crime Policy Coverage Overlaps
Selling Cyber Coverage Professional Firms

- Simplify the message
- Consider products and applications designed for professionals
- Understand the limitations of “free” endorsements
- Don’t push big limits/premiums to small firms
- Use Industry examples of exposures and claims
- Focus on the incident response and loss control service component
Non-Traditional Cyber Exposures
Beyond Data Breaches

All companies have data; but not all companies’ biggest cyber exposure is confidentiality.

To underwrite or place “non-traditional cyber” risks, you need to identify the other big types of “cyber” risk, and ensure you’re pricing/tailoring coverage for that risk.
Risk Identification

Cyber – more accurately, information security – has three aspects; think of them as “cyber perils”. InfoSec experts call this “The Triad”

- **Confidentiality:** keeping sensitive data secret
- **Integrity:** trustworthiness of the data
- **Availability:** accessibility of the data
Risk Identification

You don’t need to be a cybersecurity expert...but you need to understand these exposures to ensure you’re Underwriting/placing the coverage appropriately.

Accurate risk identification has three big benefits:

• It helps the client better understand their cyber risk, and why they need the insurance (*make the sale; and improve risk management*)

• It ensures you’re giving them the coverage they need at a fair price (*sustainable programs help both brokers and underwriters*)

• It’s a competitive advantage for your firm
Risk Identification

**Availability Example: Communications Disruptions**
Specific Example: Website/network disruption; communication with key supplier interruption
Impact: income loss & extra expense (business interruption); potential liability (SLAs)
Interesting Points: does not require a failure of security; vendor risk is a challenge

**Integrity Example: Operational or physical disruption or destruction**
Specific Example: Industrial control system takeover halting operations, breaking machinery, releasing pollutants, or destroying machinery and facilities
Impact: depends on client and service – could be a blackout, vehicle crash or even the wrong medical treatment

**Availability Example: Data Destruction**
Specific Example: Wiping data (Sony); Cryptolocker (scrambling)
Impact: depends on value of data and complexity of computer system/backups
Interesting Points: Not always caused by a failure of security – could be a systems failure
Risk Identification

“Cyber” policies don’t cover all cyber risk – especially when you start talking about integrity of data

Key limitations:
• Most cyber policies exclude bodily injury absolutely
• Most cyber policies exclude (tangible) property damage absolutely
• Most cyber policies don’t contemplate theft of insured’s monies
The Cyber Loss Spectrum
(courtesy of Axio, LLC)

Financial Damages

Physical (Tangible) Damages

1<sup>st</sup> Party Damages (to your organization)

3<sup>rd</sup> Party Damages (to others)

Losses due to cyber events (data breaches, destructive attacks, and other unauthorized access or use of your computer systems) can be categorized into these four quadrants.
2014: Germany
Cyber attack on steel mill

- Disrupted industrial control system for blast furnace
- Furnace could not be shut down
- Resulted in “massive” unspecified damage

Revealed by German Federal Office for Information Security (BSI) in December 2014. Few details are known about the event; Germans remain quiet.
Other Specific Examples

- Utility’s advanced metering infrastructure disrupted – extra expense (business interruption) incurred to roll trucks, determine usage, and send out bills

- Utilities ICS hacked causing critical assets (power generators) to overspeed, or lose phase; physical damage to assets, lost income & extra expense, etc.

- Just-in-time manufacturing facility’s ICS deleted; lost income from lost contracts (business interruption), plus costs to rebuild data (information asset coverage); potential physical loss
Coverage Solutions

• Understand client’s loss scenarios

• Manage gaps between cyber policies and their “analog” equivalents
  • Business interruption in property vs business interruption in cyber
  • Coverage for re-creation of data vs property coverage
  • Liability for data loss from mental anguish to wrongful death

• If needed, underwrite/place i) standalone cyber BI/PD policy, or ii) cyber DIC form/buyback
Takeaways

Understand your client’s cyber risk
• Research the threat environment to the client’s assets & geography
• Develop cyber risk scenarios specific to their operation
• Evaluate impact on operations and balance sheet

Examine your client’s cybersecurity program
• Use a model or framework - such as the NIST CSF – to understand what the desired outcomes of a cybersecurity program are; how does the client rank?
• Risk-based approaches work better than check-box compliance
• Do they have incident response plans (for BC/DR/Breach)? Are they practiced?
• Don’t underestimate passive safety controls!

Propose a policy that augments your client’s ability to respond to cyber attacks
• Make sure it responds to their biggest cyber risk scenarios
• Evaluate loss prevention services offered along with risk transfer
Questions?