



SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

# Cyber Liability Overview

## THE NAVAJO NATION

Presented by:  
Hilary A. Martinez  
Lavonna R. Arms

APRIL 15, 2016



# Agenda

## Understanding the Cyber Exposure

- Who is at risk
- Types of information at risk
- Where to find the risks
- Data breach timeline
- Quantifying the risk
- What are the risks

## Insurance Solutions

- Coverage overview
- Gaps and overlaps
- US insurance marketplace
- The Marsh approach
- Submission requirements
- Underwriting process

## The Future of Cyber Risk and Cyber Insurance



# Understanding the Cyber Exposure

## Who is at Risk?

Privacy, computer, and network security are not just internet issues

Any entity is at risk that transacts business using:

- a computer network
- confidential information

Industries with Higher Risk Profiles:

- Healthcare
- Retail
- Hospitality
- Financial Services
- Higher Education
- Entertainment
- Utilities

# Verizon Security Consultants 2014 Data Breach Investigations Report

92% of the 100,000 incidents analyzed from the last 10 years can be described by nine basic patterns

- Frequency of incident classification patterns by industry 2011-2013:
  - 31% Point-of-Sale Intrusions - Accommodation and Food Services, Retail
  - 21% Web App Attacks - Information, Utilities, Manufacturing, Retail
  - 8% Insider and Privilege Misuse - Public, Real Estate, Administrative, Transportation, Manufacturing, Mining
  - 1% Physical Theft and Loss – Healthcare, Public, Mining
  - 1% Miscellaneous Errors – Public, Administrative, Healthcare
  - 4% Crimeware – Public, Information, Utilities, Manufacturing
  - 14% Payment Card Skimmers – Finance, Retail
  - 15% Cyber-Espionage- Professional, Transportation, Manufacturing, Mining, Public
  - <1% Denial of Service – Finance, Retail, Professional, Information, Public

# Types of Information at Risk

## Consumer Information

- Credit cards, debit cards, and other payment information
- Social Security Numbers, Individual Tax Identification Numbers, and other taxpayer records
- Customer transaction information, like order history, account numbers, etc.
- Protected Healthcare Information (PHI), including medical records, test results, appointment history
- Personally Identifiable Information (PII), like drivers license and passport details
- Financial information, like account balances, loan history, and credit reports
- Non-PII, like email addresses and passwords, phone lists, and home address that may not be independently sensitive, but may be more sensitive with one or more of the above

## Employee Information

- Employers have at least some of the above information on all of their employees, spouses, dependents, former employees, retirees and job applicants

## Business Partners

- Vendors and business partners may provide some of the above information, particularly for subcontractors and independent contractors
- All of the above types of information may also be received from commercial clients as a part of commercial transactions or services
- In addition, B2B exposures like design plans, manufacturing plans, projections, forecasts, M&A activity, and trade secrets

# Where to Find the Risks

## A Multi-Threat Environment

### Technology

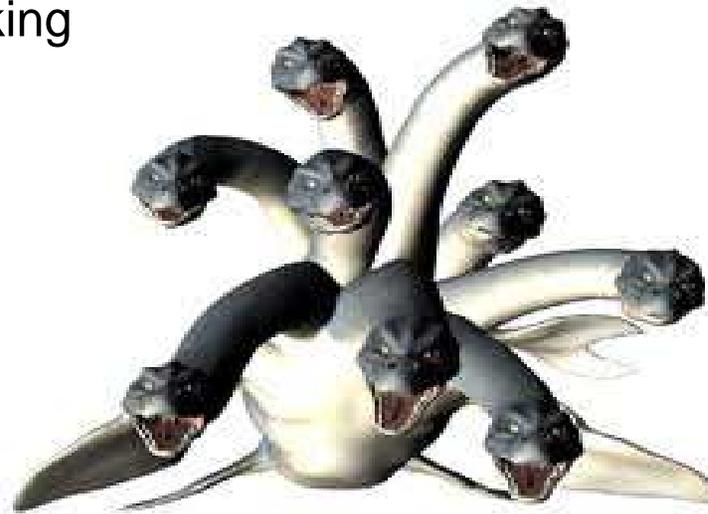
- Viruses, SQL Injections, Distributed Denial of Service attacks, etc.
- Structural vulnerability
- Social Media/Networking
  - Phishing

### External

- Business Associates
- Vendors/Suppliers (contractors, outside counsel, cloud providers)
- Foreign and domestic organized crime
- Hackers/Hacktivists

### Internal

- Rogue employees
  - Careless staff
  - BYOD



### Old School

- Laptop theft
- Dumpster diving
- Photocopier

### Regulatory

- HHS, HIPAA & HIPAA HITECH
- Identify Red Flags
- SEC, FTC, state attorney generals
- 47 State breach notification laws (NM proposed)
- PCI Compliance

# Data Breach Timeline

## Discovery

Actual or alleged theft, loss, or unauthorized collection/disclosure of confidential information that is in the care, custody or control of the Insured, or a 3<sup>rd</sup> for whom the Insured is legally liable.

Discovery can come about several ways:

- Self discovery: usually the best case
- Customer inquiry or vendor discovery
- Call from regulator or law enforcement

## First Response

Forensic Investigation and Legal Review

- Forensic tells you what happened
- Legal sets out options/obligations

## External Issues

Public Relations      Notification      Remedial Service Offering

## Long-Term Consequences

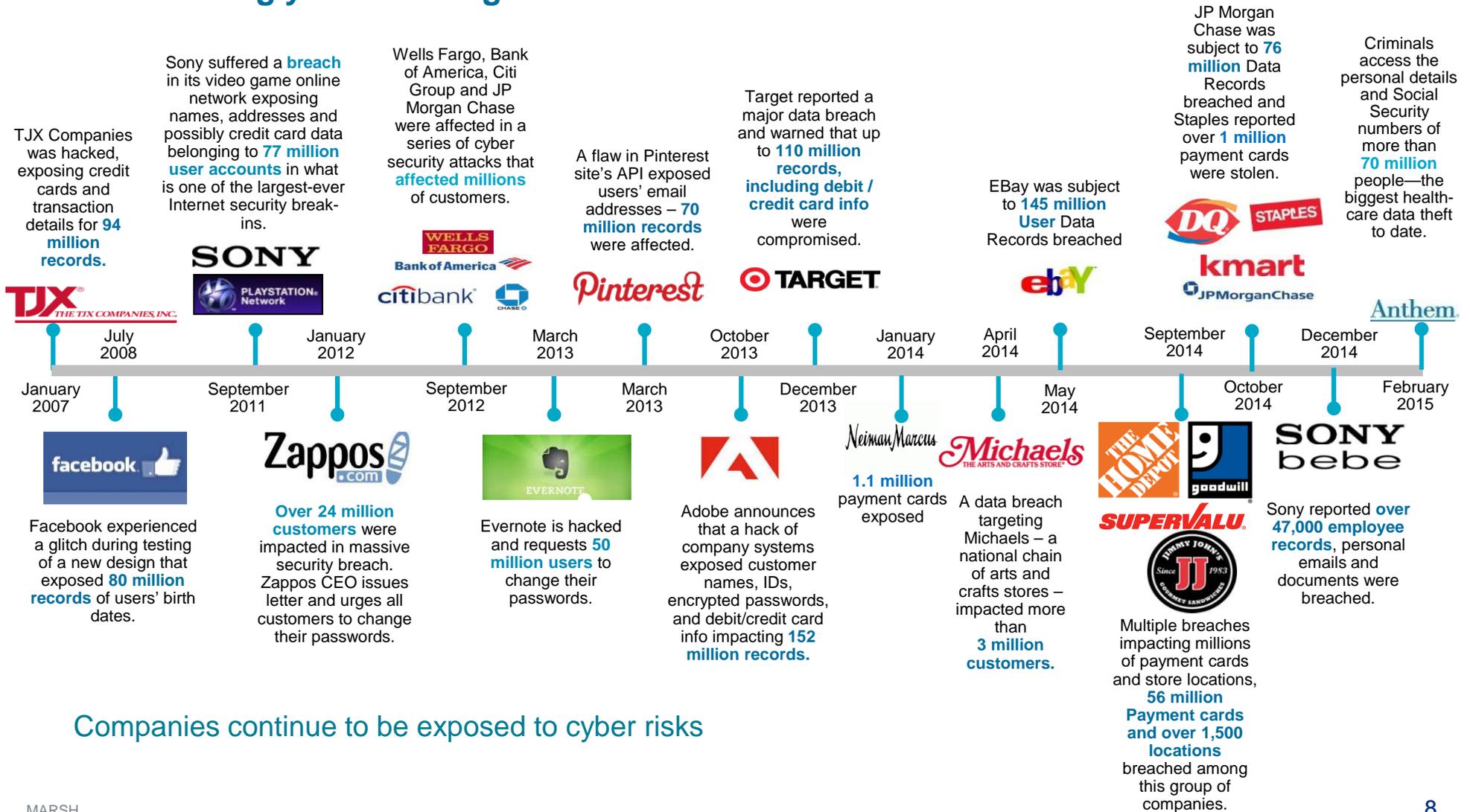
Income Loss      Damage to Brand or Reputation      Regulatory Fines, Penalties, and Consumer Redress      Civil Litigation

# Quantifying the Risk

Cost Assumptions	Insured	Insurer
Notification Costs (inclusive of legal and forensic costs)	\$2 / Record	\$.65 / Record
Call Center Costs (20% expected participation)	\$5 / call	\$2 / Call
Credit Monitoring (20% expected participation)	\$15 / record	\$8.95 / Record
ID Theft Repair (5% of those monitored experience theft)	\$500 / record	Included in the "ID Monitoring" service
Consumer Redress Fund	\$6 / record or consumer	Same
Card Reissuance (potential liability to issuers, i.e. banks)	\$6 / record	Same
Fraud Liability (range is \$500 / record to \$6,400 average fraud charges; 5% experience fraud)	\$500 / record	Same

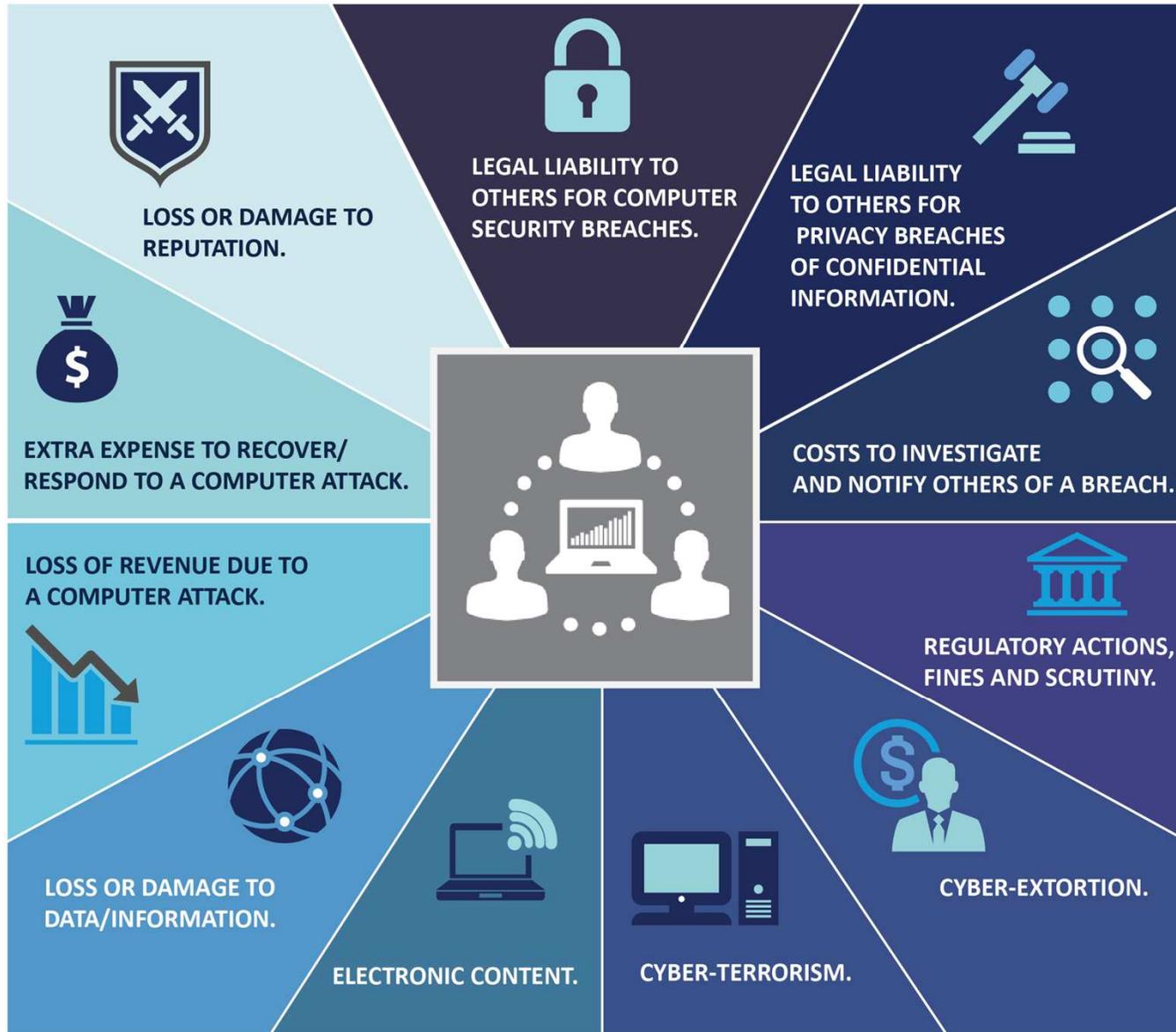
# Quantifying the Risk: Examples

## An Increasingly Threatening Environment



Companies continue to be exposed to cyber risks

# What are the Risks?



## What are the Risks?

- Legal liability to others
- Vicarious liability for acts of vendors/service providers
- Duty to comply with breach notification laws and provide credit monitoring/identity restoration costs
- Regulatory actions and scrutiny
- Cyber-extortion
- Loss or damage to data/information
- Loss of revenue/extra expense
- Loss or damage to reputation
- Stock drop or loss of market share
- Physical damage

# Coverage Overview

Coverage Part	Third Party Coverages Description
<b>Privacy Liability</b>	<p>Defense and liability for failure to keep information private or for failure of others that you have entrusted with information to keep it private (ex. pension actuary, data storage facility, credit card processor). Also includes liability for not properly notifying of a privacy breach. Coverage has expanded to include corporate confidential information and non-computer related information.</p> <p><b>Likely Claimants:</b> Customers, employees</p>
<b>Security Liability</b>	<p>Defense and liability for failure of systems to prevent spread of virus or a denial of service to those that rely on systems due to a failure in network security.</p> <p><b>Likely Claimants:</b> Customers</p>
<b>Media Liability</b> <i>Online or Full Media?</i>	<p>Defense and liability for libel, slander, disparagement, misappropriation of name or likeness, plagiarism, copyright infringement, negligence in content to those that relied on content.</p> <p><b>Likely Claimants:</b> Authors, producers, publishers, competitors</p>
<b>Technology Errors &amp; Omissions</b>	<p>Defense and liability for failure of technology products to perform their intended purpose or the failure to render technology services as intended.</p> <p><b>Likely Claimants:</b> Customers</p>

# Coverage Overview

Coverage Part	First Party Coverages Description
<b>Breach Response Costs</b>	<p>The following costs resulting from a privacy breach:</p> <ul style="list-style-type: none"> <li>• To hire computer forensics investigator</li> <li>• To hire a law firm to identify statutory obligations to notify affected individuals/regulators</li> <li>• To provide notifications</li> <li>• To setup a call center</li> <li>• To offer of fraud monitoring to those impacted individuals</li> </ul>
<b>Crisis Management / Public Relations Expenses</b>	<p>Costs of public relations firm due to privacy or security incident.</p>
<b>Regulatory Defense / Fines &amp; Penalties Costs</b>	<p>Costs to defend an action by Attorneys General, FTC, Office of Civil Rights or other regulators due to a privacy breach. Can also include associated fines &amp; penalties.</p> <p><b>Likely Claimants:</b> Attorneys General, FTC, OCR</p>
<b>PCI-DSS Assessments</b>	<p>A written demand you receive from a card association or acquiring bank for a monetary assessment of a fine or penalty due to your non-compliance with Payment Card Industry Data Security Standards (PCI-DDS).</p>

# Coverage Overview

Coverage Part	First Party Coverages Description
<b>Business Interruption / Extra Expense</b>	Loss of income or extra expense due to system shut down from security failure. Waiting period applies.
<b>Dependent Business Interruption</b>	An entity not owned, operated or controlled by you that you depend on to conduct your business.
<b>Data Restoration</b>	Costs incurred to replace, restore, or recollect digital assets from written records or from partially or fully matching electronic data records due to their alteration, corruption or destruction from a network operations security failure.
<b>Cyber Extortion</b>	Costs of consultants and extortion monies for threats related to interrupting systems and releasing private information.

# Coverage Overview

## Network Business Interruption – What Coverage is Available

- Coverage may be triggered by full or partial interruption or suspension, degradation in services or failure of a computer system – *not dependent on an external attack*
- Expenses covered include loss of income and extra expense (including forensic expense):
  - **Business Interruption** of network service due to a technology failure or an attack on the network by criminal hackers, malicious insiders/employees, distributed denial-of-service (DDoS) attacks and physical network damage.
  - **Contingent Business Interruption.** Loss of income and extra expense arising out of a network interruption caused by a service provider, web hosting companies and outsourced e-commerce service providers. (also called Dependent Business Interruption)
- System Failure coverage trigger:
  - Most policies contain a security failure coverage trigger for the business interruption coverage
  - The system failure coverage trigger expands the security failure coverage trigger to include “any unplanned outage” (examples include an administrative error or programming error)

# Coverage Overview

## Network Business Interruption – What Coverage is Available

- Data Asset Recovery:
  - Some carriers include this coverage within the Network Business Interruption coverage
  - Covers the costs and expenses incurred to restore, recreate, or recollect your data and other intangible assets (i.e. databases, software, applications) that are corrupted or destroyed by a computer attack.
- General Coverage Observations:
  - Conventional insurance products may fail to adequately address the exposures facing businesses that rely upon cloud computing services – this continues to evolve
  - Traditional property policies generally exclude cyber or non-physical perils
  - Most standard cyber policies provide small sub-limits for contingent business interruption, it is possible to schedule specific third party providers to increase sublimits
  - System failure coverage is available on a limited basis from domestic markets, more broadly available in the London market
  - Hourly waiting periods (downtime before the policy is triggered) range from 6 hours to 24 hours

# Coverage Overview

## Network Business Interruption – What Coverage is Available

- **Cause of Loss** – Is the cause of loss limited to a malicious failure in computer security or can it be extended to include accidental errors?
- **Per Hour Limitation** – Does the policy limit the maximum loss in an hour?
- **Waiting Period** – How long is the waiting period? Does it stack with the retention?  
Downtime related to cyber events is costly in a short amount of time but over fairly quickly.
- **Period of Restoration**- How long does the policy allow to get back up and running? If the site is down is there an allowance for some time after the problem is corrected for customers to come back to the site versus competitors?
- **Dependent Entities** – If the loss of income/extra expense is due to downtime of a supplier or other provider, is that covered?

# Gaps and Overlaps

Not Covered	Covered	Dependent upon specifics of claims, may have some coverage
-------------	---------	--

Cyber Perils	Property	General Liability	Traditional Crime	Computer Crime	E&O	Special Risk	Broad Privacy & Cyber Policy
Indemnification of your notification costs, including credit monitoring services							Privacy Liability
Defense of regulatory action due to a breach of privacy regulation							Privacy Liability
Coverage for fines and penalties due to a breach of privacy regulation							Privacy Liability
Threats or extortion relating to release of confidential information or breach of computer security							Cyber Extortion
Liability from disclosure of confidential commercial and / or personal information (i.e. breach of privacy)							Privacy Liability
Liability for economic harm suffered by others from a failure of your computer or network security (including written policies & procedures designed to prevent such occurrences)							Security Liability
Website infringes on IP or is defamatory							Media Liability
Destruction, corruption or theft of your electronic information assets / data due to failure of computer or network							Data Property
Theft of your computer systems resources							Data Restoration
Loss of revenue and extra expense incurred due to a failure of security							Business Interruption

## Gaps and Overlaps

- **Property:** Typically limited to damage to tangible property from a physical peril, and courts have consistently held that data isn't "property".
- **General Liability:** Covers only bodily injury and tangible property. The Personal & Advertising Injury section has potential exclusions / limitations in the area of web advertising. Now standard ISO exclusions are being added to leave no doubt that cyber risks are not covered.
- **Crime / Fidelity:** Traditionally requires intent, and is limited to theft of money, securities and tangible property. Even computer crime coverage excludes theft of data and information.
- **Professional Liability Insurance:** Even if broadly worded, still tied to "professional services", as well as requirement that there be an act of negligence.
- **Kidnap and Ransom:** Typically no coverage without amendment for "cyber extortion".
- **Fiduciary Liability:** Ensure that HIPAA civil monetary penalties are covered, and that no fiduciary liability exclusion exists for HITECH exposures.

# U.S. Insurance Marketplace

## General Commentary

### Geography

- No particular geographic buying trends in domestic market
- International purchasing is beginning to accelerate as EU Data Protection Directive and similar legislation comes online
  - Litigation environment still not on par with more aggressive U.S.

### Client Size

- Market was historically driven by large risk, but middle-market and small client space are increasing exponentially
- Small client space is increasingly being serviced by MGA's and group purchasing facilities (programs)

### Industry

#### Key Industries

- Healthcare
- Retail
- Hospitality
- Financial Services
- Higher Education
- Entertainment
- Utilities

#### Newly Interested

- Manufacturing
- Industrial
- Critical Infrastructure

# U.S. Insurance Marketplace

## No Capacity Crunch

- Capacity, Coverage, and Cost are the three sides of the insurance triangle.
- Coverage continues to expand.
  - Increased uptake of first party coverages
  - Expanding coverage for PCI breaches
  - Continued carrier innovation
- Capacity remains available.
  - Marsh's recent survey of capacity for large purchasers indicates \$350M+.
  - More capacity is available if cyber is blended with E&O (where appropriate).

# U.S. Insurance Marketplace

## Recent Trends

### Cyber Market Update – 4thQuarter 2015

#### Key Highlights for 4th Quarter 2015

The market's response to high profile cyber losses is now reflected in the structure and pricing of cyber programs. Average price increases, not including the retail and healthcare sectors, have increased 7.9%. Whereas average price increases for the retail sector have increased 56.7%. This drastic change is likely a direct result of the recent frequency and severity of retail cyber losses. Further, average price increases for the healthcare sector have increased 12.5%, up from a 6.9% increase last quarter. While this sector's increase is not as significant as the retail sector (yet), we think it's because the frequency and severity of healthcare cyber losses didn't turn until 1/3 of the way through the 1<sup>st</sup> quarter, hence the market is still actively responding. Recently we have seen the healthcare sector experience similar changes to program structure and pricing as the retail sector, particularly in the managed care space. It's important to note that competition remains fierce for non-retail exposed risks.

#### Claims Trends

There have been continued high profile cyber data losses, most notably in the retail and healthcare sectors. That said, the surge in interest in cyber coverage continues. We see first-time buyers enter the market at a more rapid pace than in the past, as well as existing buyers increase their limits, sometimes at double the expiring limits. Marsh's proprietary Cyber IDEAL model is also providing clients with a better understanding of their exposures and helping them in deciding appropriate risk transfer choices.

# U.S. Insurance Marketplace

## Recent Trends

### Cyber Market Update – 4th Quarter 2015 cont'd

#### Insurance Market

Overall capacity remains abundant at \$200–\$400 million, depending on the insured's class of business, as well as the cyber coverage options elected for purchase. There have been no significant new entrants in the last quarter, but individual insurer appetite has changed significantly, with a handful of markets either leaving the stand-alone cyber arena altogether or restricting their appetite to certain attachment points, deployed limits, followed coverages, etc. Also note the announcement of ACE's acquisition of Chubb, which we are monitoring closely.

#### Other Issues for Consideration

Infrastructure / manufacturing clients continue to show heightened interest in business interruption coverage. Sublimits for the various cyber coverages (e.g. Privacy Notification Costs and Regulatory Costs) are still trending up, with many clients exploring renewal options with sublimits and no sublimits. Further, insurance requirements from our insureds' customers continue to increase in scope and specificity with relation to cyber, which is also driving some buying behavior.

## The Marsh Approach

- **Placement of coverage is the last step in the process**
- Insurance is a complement to good risk management
- Technology is not a “silver bullet” that will defend against all risks; prevention is not enough.
- Marsh’s approach to the privacy and cyber risks combines:
  - Assessment;
  - Education;
  - Preparation; and
  - **Risk transfer.**

## Submission Requirements

- Completed application
- Loss runs
- Depending on industry or services provided, supplemental applications may be required
- Depending on industry or services provided, an underwriter call may be required

# Submission Requirements

## Sample Cyber Call Questions

### Security Organization

- Which group is primarily responsible for information security at Company X? Who leads this group, and how do they report up (to the CIO, BoD, etc?)? How many FTEs are in this group today? How much turnover has there been in the group?
- What people, positions or groups within Company X have a voice in the Information Security posture of the organization?
- How does Company X's infosec team digest all of the various alerts, logs and other information sources? What sort of Security Information and Event Management tool are they using, and who is responsible for investigating alerts (is there a Systems On Chip or Network On Chip) – is a Managed Security Service Provider involved)? How are these processes tested and validated?
- Describe any company-wide programs to train staff in privacy and security related matters, including phishing, identity theft, and social media.
- What is the turnover within the groups responsible specifically for information security (vs the larger IT)? How much is headcount growing, and how are you finding people with the right skills and background?

# Underwriting Process

## Best Practices: Type of Records and Loss Experience

### Information on Records

- Number of records (PII, PHI, PCI)
- How and where is it stored?
  - On site?
  - Third party vendors?
  - Public/private cloud?

**Best Practice:** Confidential information is encrypted at-rest, in-transit, and on portable devices; access to sensitive data is restricted on a role or business need basis; PII reduction program is in place where applicable

### Loss Experience

- Have there been any cyber events in the last year?
- How many and how much information has been exposed?

**Best Practice:** If the applicant has experienced a data breach or privacy event, steps have been taken to mitigate against future events/losses

# Underwriting Process

## Best Practices: Compliance and Controls

### Regulatory Compliance

- **Best Practice:** Compliant with all regulatory rules/statutes that may govern the industry in which the client operates

### Organizational & Administrative Controls

- **Best Practice:** Formal policies and a framework is in place for data protection that is communicated to all employees and has been reviewed by a qualified attorney; an established security team structure wherein IT management/data security is separate from IT operations; designated individuals or committees with oversight and responsibility over IT security and privacy

### Electronic Controls

- **Best Practice:** Updates and patches to security software are completed in a timely manner and proactively monitored; vulnerability scans are performed on all critical systems and deficiencies are properly mitigated and addressed

### Physical Security Controls

- **Best Practice:** Access to static data (file rooms/backup tapes) and servers is restricted to authorized employees at specified entry points

# Underwriting Process

## Best Practices: Culture, Planning, and Preparedness

### Security and Privacy Culture

- **Best Practice:** Network security and data privacy is a board level concern; employees are educated and aware of the importance of data security and understand their personal liability for participating in a data breach incident

### Crisis Management Preparedness

- **Best Practice:** a pre-planned and well documented incident response plan and escalation plan is in place and enforced

### Business Continuity/Disaster Recovery Planning

- **Best Practice:** A business continuity and incident response plan is in place, reviewed tested, and updated continually, and communicated to employees; redundancies are in place to prevent against a total and permanent loss of data/information;

# What's in Store for the Future



Thank You!

