CYBER LIABILITY SYMPOSIUM

June 1, 2017

Seattle, Washington

Panelists

Adam Butera, RPLU, Travelers Bond & Specialty Insurance

Jeff Costlow, ExtraHop Networks

Sean Hoar, Lewis Brisbois Bisgaard & Smith LLP

Andreas Kaltsounis, Stroz Friedberg

Special Agent Briana Neumiller, FBI Seattle Cyber Division

Moderators

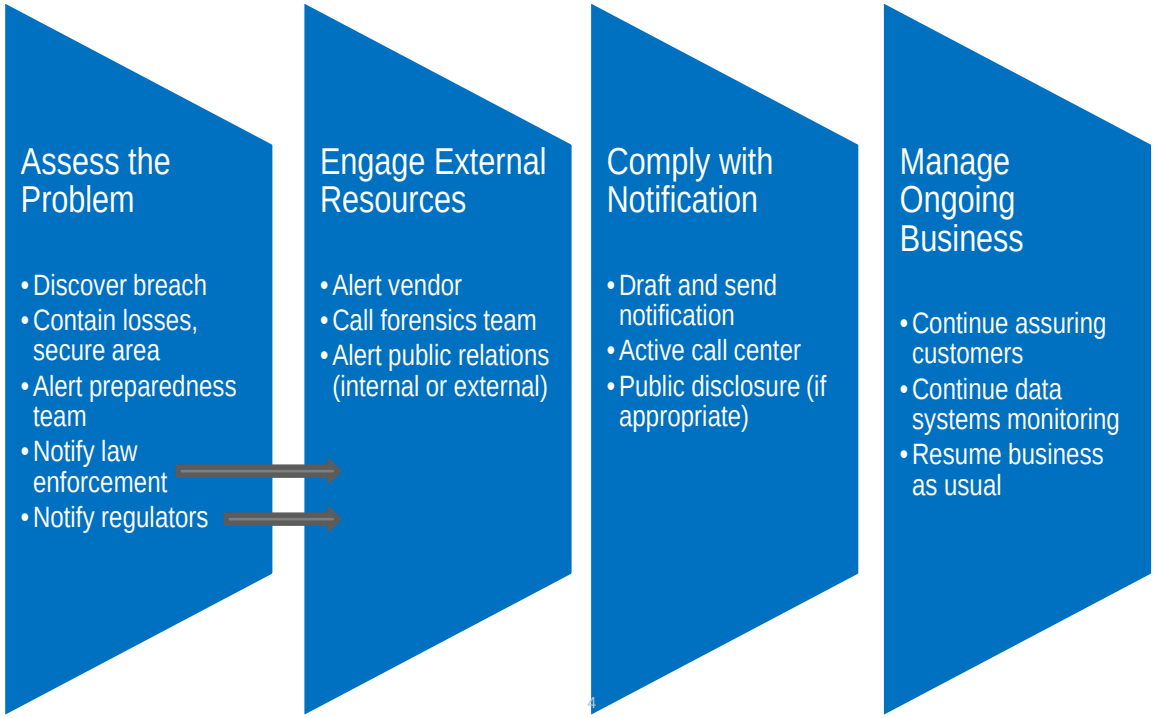
Michael Handler, Cozen O'Connor

Peter Marchel, Marchel & Associates Risk Consulting

Agenda

- Trends in Cyber Liability and Data Breaches
  - What's happening now
  - Who's paying the price
- Pre-Breach Preparedness
  - What can you do to prepare
  - How will it help
  - What to look out for
- Applying Cyber Insurance Resources
  - How insurance policies respond to cyber events

Data Breach Life Cycle



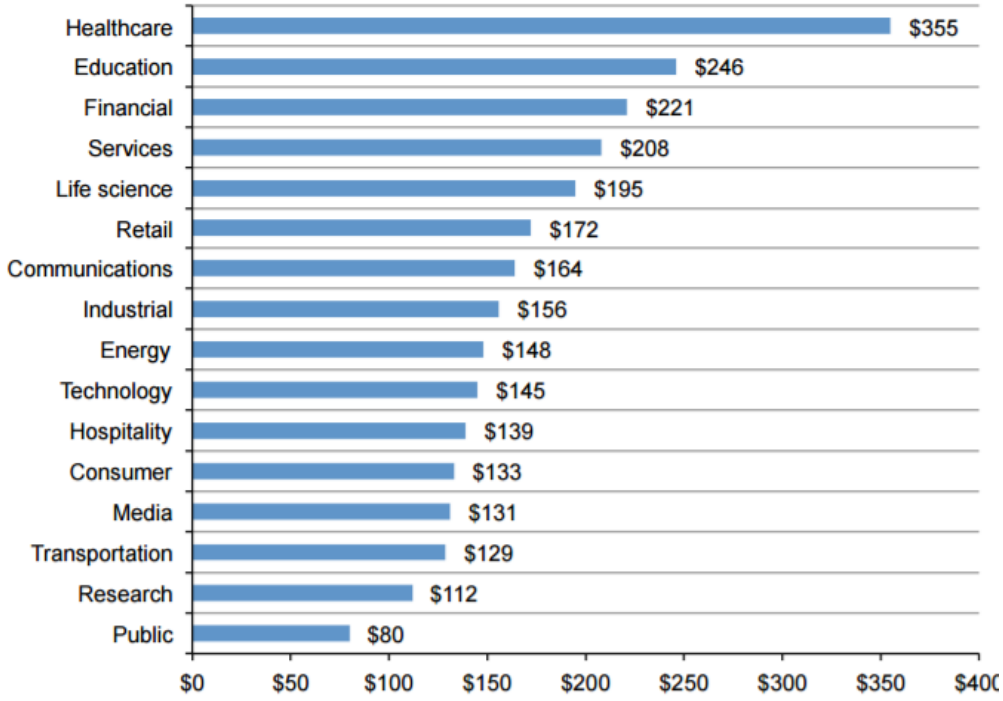
WHAT ARE THE NUMBERS?

I. Ponemon Institute (2016 report):
   a. $4M – Avg cost per data breach
      - 2015 Average Cost: $6.53 Million

   b. $158 (USD) – Avg. cost per record
      - 2015 cost per record was $217 (USD)

   c. $7.01M – Avg. annualized cost of US cybercrime per organizations

II. Causes of Compromise:
   a. 48% - malicious/criminal attacks
      - $170 avg. cost per record
   b. 25% - negligence/human error
      - $133 avg. cost per record
   c. 27% - system glitches
      - $138 avg. cost per record



The cost of a data breach can vary significantly by industry, due to differences in the types of data collected and various regulatory and compliance obligations:

A recent study showed that healthcare currently expects the largest cost, at an average of $355 per record.

Note these numbers contemplate both the insurable costs of dealing with a data breach, including notification, credit monitoring, lawsuits, and regulatory fines, as well as less-quantifiable costs such as reputational harm and loss of future revenue.

Data Breach Costs Per Sector

Source: 2016 Cost of Data Breach Study: Global Analysis
Sponsored by IBM, Conducted by Ponemon Institute LLC

WHAT ARE THE NUMBERS?

Mandiant's Mtrends 2017: A View From the Front Lines

a. Compromise detection victims notified by external entity 47%.
b. 99 days median number of days threats were present in a victim's network before detection.
    a. 2015 Mtrends survey's median number: 205 days

VICTIMS BY THE NUMBERS

- M Trends (2017):
  - 15% - Retail
  - 15% - Financial Services
  - 10% - Business & Professional Services
  - 12% - High-Tech & IT
  - 12% - Healthcare
  - 8% - Government
  - 5% Manufacturing
  - 5% - Media & Entertainment (down from 13%)
  - 3% - Construction & Engineering
  - 2% - Transportation & Logistics

The Cyber Kill Chain® framework:

- **Step 1: Reconnaissance**
- **Step 2: Weaponization**
- **Step 3: Delivery**
- **Step 4: Exploitation**
- **Step 5: Installation**
- **Step 6: Command and control**
- **Step 7: Action on objectives**

Source: Lockheed Martin Corp.

The Cyber Kill Chain® framework – Real World Variations

- Research and development on the hackers' side is funded by crowd-sourced ransom amounts.
- Hackers' game plans, and insider threats, that shortcut the "Kill Chain" links
- Law enforcement's goals & the affected organizations' goals.

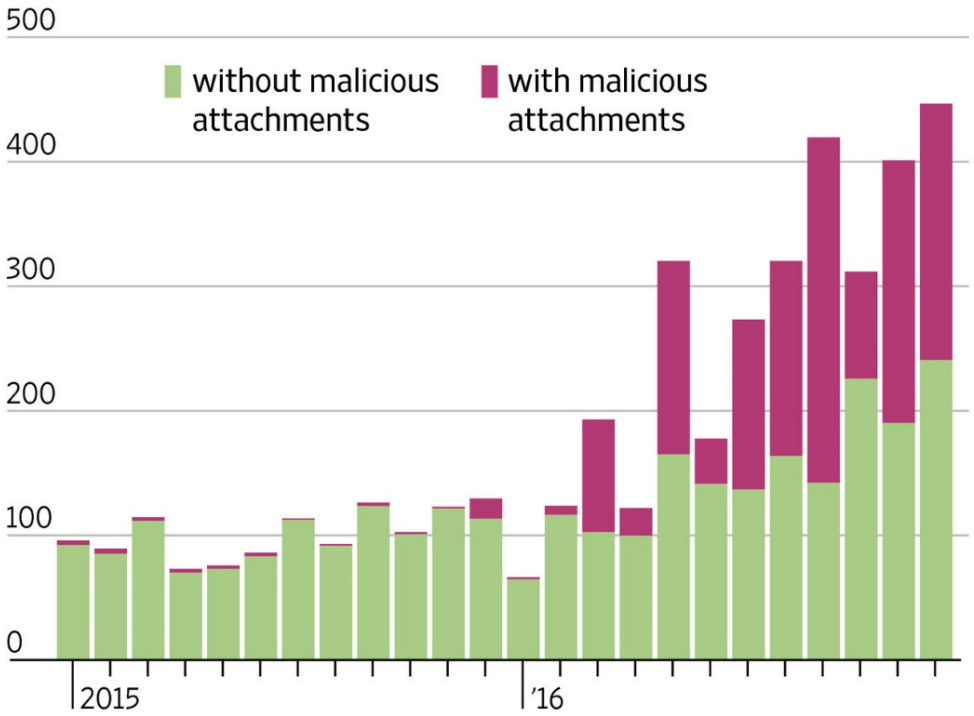
Training

- Training brings awareness to likely attack vectors.
- Training establishes compliance and reduces risks.
- Training will not be 100% effective.
- Risk Specific Training
  - Table Top Training
  - Social Engineering
  - Breach Simulation

Don't Open That Attachment

The past year has seen a meteoric increase in emails around the globe containing malware, according to a recent IBM Security study.

Change in amount and type of spam email, 1Q 2015 = 100



Source: IBM X-Force

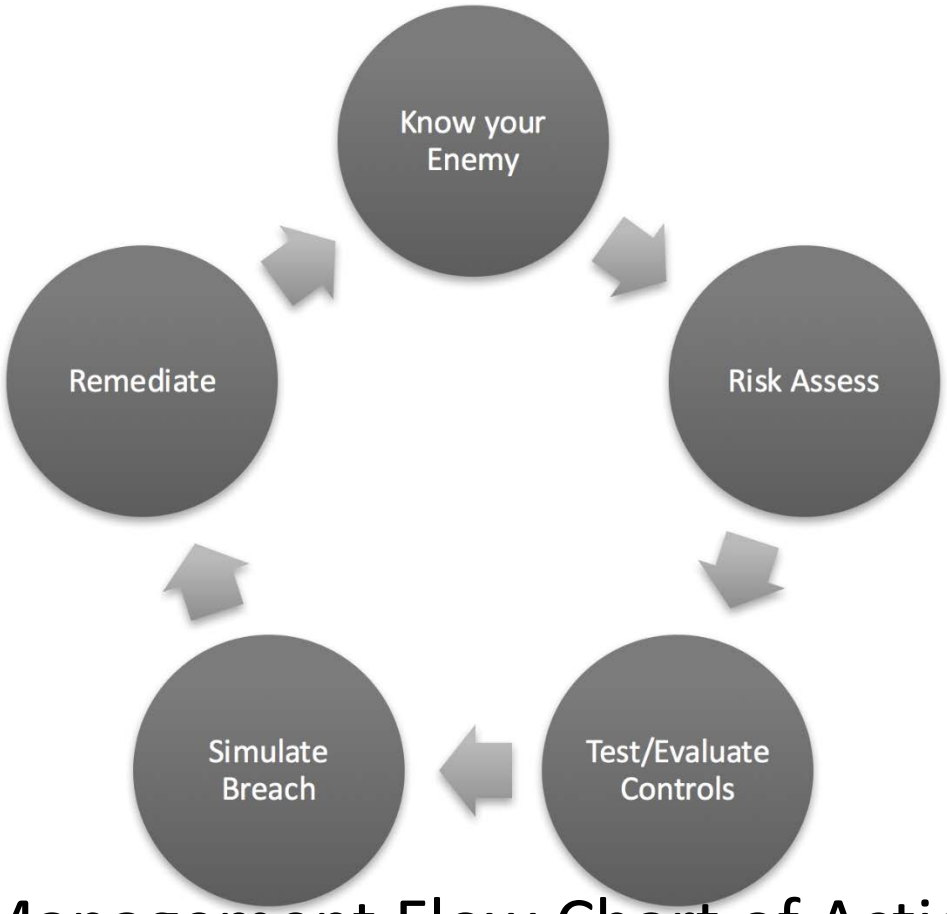
THE WALL STREET JOURNAL.

Tips From The Pros – Anticipating The Threats

- People
- Process
- Technology

Planning to Respond

- Develop a tailored, written plan that identifies your response team and their jobs
- Identify the resources needed to implement
- Test
- Update



Risk Management Flow Chart of Action Steps

What type of Data resides on these servers?

- What difference does it make if you have:
  - PII
  - PHI
  - PCI
  - DSS
  - Other

- What are your obligations regarding affected **personally identifiable information (PII)**?
  - Data breach notification statutes require immediate notification of consumers whose unencrypted PII has been acquired without authorization.
  - The definition of PII varies from state to state, but generally includes a first name or first initial and last name of a person, in combination with one or more of the following data elements:
    - Social Security number;
    - driver's license number or state identification card number;
    - Account number or credit or debit card number and the means to access the account;
  - Some states also include as PII medical information, health information, online user credentials with the means to access the account, and/or biometrics.
  - While all states require immediate notification, a number also include an outside time frame for notification. As an example, Washington requires notification as expeditiously as possible, but no later than 45 days from discovery of the breach.
  - A number of states also require notification of a regulatory official if consumers are affected. As an example, Washington requires notification of the state Attorney General if more than 500 Washington residents are affected.

- What are your obligations regarding affected **protected health information (PHI)**?
  - The Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule requires a covered entity (health care provider, health plan, or similar health care entities) to notify individuals whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed in violation of the HIPAA Privacy Rule.
    - PHI is defined as any "individually identifiable health information" that is transmitted or maintained in any medium, electronic or otherwise.
      - Health information includes any information that is created or received by a covered entity that relates to the past, present or future physical or mental health of an individual, the provision of or payment for health care to that individual
  - The notice must be made without unreasonable delay and no later than 60 calendar days after the breach is discovered.
    - If more than 500 individuals have been affected within a geographic jurisdiction, media notice is also required within 60 days of the discovery of the breach.
    - If more than 500 individuals have been affected, regardless of their geographic concentration, the Secretary of the Office for Civil Rights must also be notified within 60 days of the discovery of the breach; otherwise the notice must be provided within 60 days of the end of the calendar year in which the breach was discovered.

What are your obligations regarding affected **payment card industry (PCI)** data?

- Obligations under the PCI Data Security Standard (PCI DSS) are determined by contract with merchant banks and card brands.
  - Notice to merchant banks and card brands is generally required within 24 hours of discovery of the compromise of PCI data.
- Upon notice to card brands, the breached entity may be required to engage a PCI certified forensics investigator (PFI) from a list maintained by the PCI Council.
  - If this occurs, the PFI typically must be engaged within three business days.
  - The breached entity will bear all costs of the forensics investigation.
- Within four days of the notice to the card brands, an incident report or incident time line will typically be required from the card brands.
- Expenses for card replacements and fraud loss will be passed on to the breached entity by the card brands.

Discussion: Who to Notify? And When?

- Incident Response Team
- Marketing
- Employees
- Clients
- Regulators
- Law Enforcement Agencies (FBI, Secret Service)
- Incident Reporting Agencies
- Board of Directors
- Media
- Legal
- Vendors
- Business Partners
- Internet Service Providers
- Insurance Provider
- Other organizations identified by team members.

Notifications and Stakeholder Communications

- Who should be contacted?
  - Internally
  - Externally
- How quickly should communication occur with key stakeholders?
- What do you tell your stakeholders?

Organizational Differences and Additional Considerations

- Publicly traded
- Private Company
- Governmental Entity
- Non-profit entity

Types of Data Breach Costs

- FIRST PARTY LOSS
  - **cyber extortion**:
    - **payment to criminals** that have installed “ransomware” on a system and proceeded to encrypt everything connected to the point of entry – in order to have the system decrypted;
    - **forensics examination** to ensure that the ransomware attack wasn’t a subterfuge to install additional malware on the system;
    - **legal analysis** to determine whether the attack constituted a reportable breach under data breach notification statutes or regulatory schemes;

  - **other computer crime loss** which may involve the following costs:
    - money lost through computer fraud or funds transfer fraud – hacker infiltrates a network and uses a combination of social engineering and technical subterfuge to steal money.

Damage to the Business

- **Breach Notification**
- **Immediate Costs**
  - **data loss -** valuable data processed, transmitted and/or stored – which may be PCI, PHI, proprietary, employment, etc.
  - **software loss -** the corruption or destruction of applications
  - **hardware loss -** damage to servers, routers, printers, laptops, mobile devices and anything which may be part of the network share
  - **remediation costs**;
  - **business interruption / extra expense**;
  - **restoration costs**;

Damage to the Business

- **Multiple Avenues of Continuing Loss**
  - Regulatory Fines
  - Litigation (Government and Private actions, Class Action)
  - Loss of Reputation
  - Loss of Productivity
  - Loss of System Availability
  - Loss of Intellectual Property

- **Loss of Reputation**
  - Required public notice to involved consumers
  - Press and internet (blogs, et al.)
  - Government (Attorneys General…etc.)

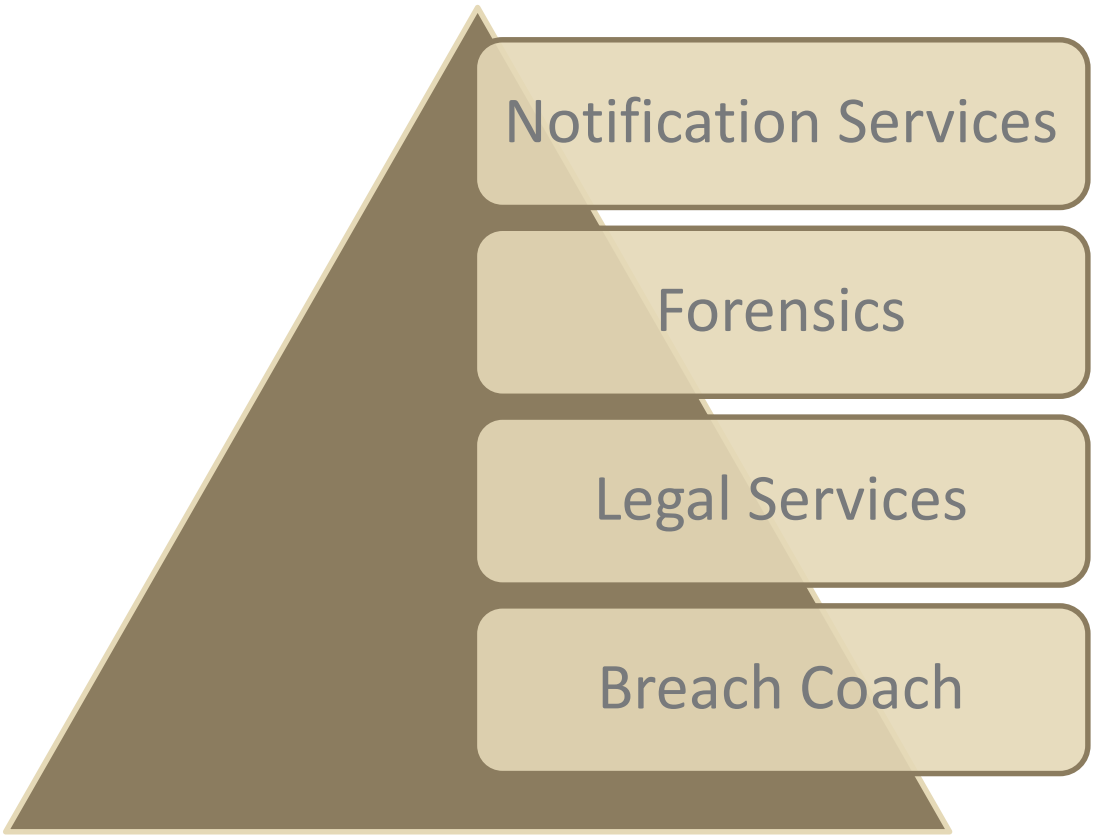
Damage to Others

- **Affected Individuals**
  - Fraudulent debts and accounts
  - Late fees/overdraft fees for drained accounts
  - Harm to credit score
  - Tax fraud
  - Medical fraud
  - Time and attention to fix
  - Worry
- **Shareholders:** Loss of value
- **Banks/Credit card companies**
  - Cost of fraudulent charges
  - Card re-issue costs

Who Can Sue?

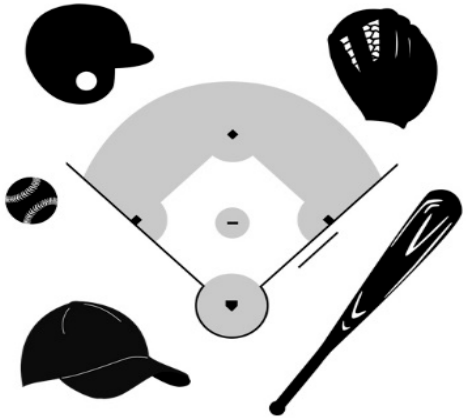
1. **Customers**
   - Need actual out of pocket damages (unreimbursed charges, late fees, credit monitoring)—or maybe not
   - Standing is an on-going battle, more easily met in the 9th Circuit
   - Plaintiffs are constantly trying new strategies
2. **Shareholders**
   - Allege that Board's failure to pay sufficient attention to cybersecurity caused breach
3. **Credit card Issuers**
   - Claim costs of reissuing cards

Cyber Coverage = Access to Resources



Insurance Coverage for Data Breach Events

- **First Party Coverage**
  - Damage to digital assets
  - Business interruption
  - Extortion
  - Privacy Breach Expenses
- **Third Party Coverage**
  - Privacy liability
  - Network security liability
  - Internet media liability
  - Regulatory liability
  - Contractual liability



First & Third, Nobody Out?

ISO EXCLUSION FROM CGL POLICIES– DISCLOSURE OF INFORMATION

- Coverage A: 2014-adopted exclusion reads in part…

Exclusion – Access or Disclosure of Confidential or Personal Information and Data-Related Liability – With Limited Bodily Injury Exception -- *CG 21 06 05 14*

"Damages arising out of:

(1) Any access to or disclosure of any person's or organization's **confidential or personal information**, including…trade secrets,…financial information, credit card information, health information or **any other type of nonpublic information**; or

(2) The loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."

ISO EXCLUSION FROM CGL– DISCLOSURE OF INFORMATION

- Coverage B: 2014 exclusion reads in part…

" 'Personal and advertising injury' arising out of any access to or disclosure of any person's or organizations' **confidential or personal information**, including patents, trade secrets,…, customer lists, financial information, credit card information, health information **or any other type of nonpublic information**." (emphasis supplied)

Risk Shifting By Agreements With Vendors, Others

-Understand where data resides, Understand who has access.

-Understand liability typically follows the owner of the data

-Establish relationships externally or internally

to prepare for pre- and post-breach

-Clarify terms in contractual arrangements:

-- vendor will indemnify / hold harmless; or

-- vendor will maintain cyber insurance.

Factors When Considering Policy Limits

- How many records does the insured have?
- Size and location of the insured and its customers.
- Customer profile.
- Does the cyber policy have separate limits or are the limits shared with / “stacked” with other coverages (management liability, employment liability, professional liability)?
- Self Insured Retention amounts.

33

Timely Notice to Insurers –

- Key Benefits – providing first responder, providing expertise & resources.
- Coverage implications – e.g., all Related Claims, whenever made, are deemed to be a single Claim and to have been first made at the earliest notice date.
- Impact of Self Insured Retentions.

Insurer Communications

- Setting up protocols:
  - Interfacing with the insurers and counsel
  - Communication, billing, etc.
- Resolution of coverage issues or dispute
  - Involving brokers and/or intermediaries in claims tender, response to RFI and ongoing facilitation.
- Strategies for mitigating transactional costs

“Prioritizing” Among Insurers

- Insurers Timely Responding to Insured
- Insurers Timely Cooperating With Each Other:
  - Cyber/Data Breach insurer, Professional Liability, Directors & Officers Liability, Multimedia Liability & Advertising injury, all potentially have shares of liability insurance obligations.
  - Insureds with interests in retaining their limits for uncertain future exposures may have incentive to target, monitor or direct cooperating insurers.
- Strategies for mitigating transactional costs

Key Takeaways - Insurance

- Know your insurance program.
- Know your limits and retentions.
- Review policy and limits annually.
- Know how to report a claim.
- Know how to interact with the insurance companies.

37

Panelists

- Adam Butera, RPLU, Travelers Bond & Specialty Insurance, abutera@travelers.com
- Jeff Costlow, ExtraHop Networks, costlow@gmail.com
- Sean Hoar, Lewis Brisbois Bisgaard & Smith LLP, Sean.Hoar@lewisbrisbois.com
- Andreas Kaltsounis, Stroz Friedberg, AKaltsounis@StrozFriedberg.com
- Special Agent Briana Neumiller, FBI Seattle Cyber Division, Briana.Neumiller@ic.fbi.gov

Moderators

- Michael Handler, Cozen O'Connor, mhandler@cozen.com
- Peter Marchel, Marchel & Associates Risk Consulting peterm@marchelassociates.com