CYBER LIABILITY
SYMPOSIUM

April 21, 2016
Seattle, Washington
Panelists

• Amelia Gerlicher, Perkins Coie LLP
  206.359.3445 | agerlicher@perkinscoie.com

• Jason Glasgow, Travelers Insurance
  860.277.4231 | jglasgow@travelers.com

• Tom Schauer, CliftonLarsonAllen
  253 468 9750 | tom.schauer@claconnect.com

• Timothy Wallach, Supervisory Special Agent, Cyber Task Force, FBI
  206.287.3601 | Timothy.Wallach@ic.fbi.gov

Moderator

• Michael D. Handler, Esq., Cozen O’Connor
  206.808.7839 | mhandler@cozen.com
Agenda

• Trends in Cyber Liability and Data Breaches
  – What’s happening now
  – Who’s paying the price
  – How does insurance fit in

• Pre-Breach Preparedness
  – What can you do to prepare
  – How will it help
  – What to look out for
Trends in Cyber Liability / Data Breaches

What organizations have “Cyber Risks”?

*All of them.*

Any organization that:

1. uses technology in its operations, or

2. handles/collects/stores confidential information—including employee information.
“In the world of networked computers every sociopath is your neighbor”

-Dan Geer
• Trending Threats

  – Ransomware
  – Business Email Compromise
  – Banking Malware/Trojans
  – Point-of-Sale Malware
  – Employee Accidents, Errors and Omissions
• Breach Facts
  – “Amateurs hack systems, professionals hack people.” - Schneier

  – Breach Gain: $5/record when selling financial identity
    
    60,000 customers = $300,000 Gain to Attacker

  – Breach Cost: $80 to $200 per record
    
    60,000 customers = $4,800,000 Loss to Victim
WHAT ARE THE NUMBERS?

• Ponemon Institute (2015):
  – $6.53M – Avg. cost per data breach
  – $217 (USD) – Avg. cost per record
  – $15M – Avg. annualized cost of US cybercrime per organizations
  – 160 – Avg. successful attacks on organization per week

• Causes of Compromise:
  – 49% - malicious/criminal attacks
    • $230 avg. cost per record
  – 19% - negligence/human error
    • $198 avg. cost per record
  – 32% - system glitches
    • $210 avg. cost per record

• Note: Ponemon excludes breaches exceeding 100k records from its analysis. Breach range from 2015 was 5,000 to 100,000 records.
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 $359 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.

Source: 2014 Cost of Data Breach Study: Global Analysis
Sponsored by IBM, Conducted by Ponemon Institute LLC
Evolving Threat Trends: Top 5 Threats to Data - and Cyber Security

I. Breach from External Threat (80%)
II. Phishing 23%, 11% open attachments
III. Spyware/Keylogger 5%
IV. Ram Scrapper 20% (largest increase)
V. Credentials 52%

Verizon 2015 Data Breach Investigations Report
WHAT ARE THE NUMBERS?

- Verizon’s 2015 Data Breach Investigative Report questions the prior figures used by other organizations in calculating the cost per record breached. The following are Verizon’s figures based upon their revised model for predicting exposure.

<table>
<thead>
<tr>
<th>Records</th>
<th>Average (low)</th>
<th>Expected</th>
<th>Average (upper)</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>$18,120</td>
<td>$25,450</td>
<td>$35,730</td>
</tr>
<tr>
<td>1,000</td>
<td>$52,260</td>
<td>$67,480</td>
<td>$87,140</td>
</tr>
<tr>
<td>10,000</td>
<td>$143,360</td>
<td>$178,960</td>
<td>$223,400</td>
</tr>
<tr>
<td>100,000</td>
<td>$366,500</td>
<td>$474,600</td>
<td>$614,600</td>
</tr>
<tr>
<td>1,000,000</td>
<td>$892,400</td>
<td>$1,258,670</td>
<td>$1,775,350</td>
</tr>
<tr>
<td>10,000,000</td>
<td>$2,125,900</td>
<td>$3,338,020</td>
<td>$5,241,300</td>
</tr>
<tr>
<td>100,000,000</td>
<td>$5,016,200</td>
<td>$8,852,540</td>
<td>$15,622,700</td>
</tr>
</tbody>
</table>
AVERAGE NUMBER OF MALWARE EVENTS PER WEEK FOR 5 INDUSTRIES:

I. Financial Services (350)
II. Insurance (575)
III. Retail (801)
IV. Energy/Utilities (772)
V. Education (2,332)

Verizon 2015 Data Breach Investigations Report
WHAT ARE THE NUMBERS?

Mandiant’s Mtrends 2015: A View From the Front Lines

a. Compromise detection victims notified by external entity 69%.

b. 205 days median number of days threats were present in a victim's network before detection.
VICTIMS BY THE NUMBERS

• M Trends (2015):
  – 17% - Business & Professional Services
  – 14% - Retail
  – 10% - Financial Services
  – 8% - Media & Entertainment (down from 13%)
  – 8% - Construction & Engineering
  – 7% - Government & International Organizations
  – 7% - Legal Services
  – 7% - High-Tech & IT
  – 6% - Healthcare
  – 5% - Transportation
Damage to the Business

- **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
  - **income loss**;
  - **business interruption costs**;
  - **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 most easily met in the 9th Circuit
   - Plaintiffs are constantly trying new strategies

2. Shareholders
   - Alleges that Board’s failure to pay sufficient attention to cybersecurity caused breach

3. Credit card Issuers
   - Claim costs of reissuing cards
Legislating the Issue

- **Federal Government** – 5+ major statutory schemes
- **State Laws** – At least 47 states
  - Notification laws
  - Requirements to secure data

**Example Notification Statute:**

- Any person or business that conducts business... shall disclose any breach of the security of the system following discovery... The **disclosure shall be made in the most expedient time possible, no later than 45 days after the breach was discovered**...

Regulating the Issue

• FTC’s Generalized Regulations Across Multiple Industries
• A Sea of Industry-Specific Regulations
  – GLBA: Financial Institutions
  – HIPAA: Healthcare
  – FERPA: Education
  – NERC: Energy and Critical Infrastructure
  – FISMA: Federal Government
  – PCI-PIN and PCI-DSS: Payment Card Industry

• Generally based upon NIST.
• Use an accepted standard to guide your infosec program
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?*
Insurance Coverage for Data Breach Events

What is Cyber Publication?


- Old fashioned reel to reel computer tapes – with IBM employee info – fell off of a truck. Never recovered.

- No “publication” because “[A]ccess is a necessary prerequisite...” and plaintiffs failed to show that “information on the tapes was ever accessed by anyone.”

- NOTE: No access because data encrypted, and only IBM’s proprietary program could retrieve data. This is rare case where loss of data will not be “publication.”
Insurance Coverage for Data Breach Events

Sony PlayStation Ruling (NY Trial Court, February 2014)

- Coverage B: “oral or written publication in any manner of material that violates a person’s right of privacy”
- Issue: whether Sony required to commit the breach-causing act, or if third parties’ acts suffice
- Court found Sony was not involved in the “publication” – declined to expand insurer’s liability by construing “in any manner” to include criminal hackers
- Provision could only be read to require policyholder to perpetrate or commit the “publication” - could not be expanded to third parties
- Implications: otherwise reluctant policyholders encouraged to buy data breach coverage
- No automatic coverage for these types of large-scale response costs, or responding to third party litigation
US Courts of Appeals for the Eighth, Ninth, and Tenth Circuits have found coverage for computer, cyber, and privacy risks under traditional CGL policies.


- Computer user alleged Eyeblaster injured his computer, software, and data after he visited Eyeblaster website.
- Eyeblaster tendered defense to insurer, seeking coverage under CGL policy and an Information and Network Technology Errors or Omissions Liability policy. Insurer denied insured’s defense.
- **Held:** Software explicitly excluded, but computer is tangible property ...

Fourth Circuit Court of Appeals, Travelers Indemnity Co. of America v. Portal Healthcare Solutions LLC, Unpublished Decision issued April 11, 2016:

- Duty to Defend class action based on allegations Portal negligently failed to secure its server containing confidential records of patients at a hospital.
- Coverage B “publication” by Portal occurs when information “is placed before the public,” not if/when someone reads it.
ISO EXCLUSION – DISCLOSURE OF DATA

- Coverage A: Recently adopted exclusion reads in part...

Exclusion – Access or Disclosure of Confidential or Personal Information and Data-Related Liability – With Limited Bodily Injury Exception

“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 – DISCLOSURE OF DATA

- 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,...financial information, credit card information, health information or any other type of nonpublic information.”
“HACKING” THE EXCLUSIONS?

- What about a data breach where the information is public, but disclosure can harm someone?
  - Eg. -- List of embarrassing items customer purchased while physically in a public store.
  - Eg. -- An attorney who has a list of all claims/lawsuits made against a client. (Eg. Product liability claims.)
  - **NOTE:** Attorney has duty of confidentiality, even as to public information about client.

- While information is public, ability to gather the info and/or to target a person was made easy by the breach.

- The problem is with trying to anticipate the nature of a risk that is quickly changing, and almost unimaginable in scope.
Cyber Coverage = Access to Resources

- Notification Services
- Forensics
- Legal Services
- Breach Coach

www.marchelassociates.com | proprietary & confidential
Underwriting to Rapidly Evolving Exposures

- Education/Training
- Claim experience; why carriers ask questions
- Listen to Insureds
- Dynamic exposures  ---> Dynamic coverage
Factors When Considering Policy Limits

• How many records does the insured have?
• Does the cyber policy have separate limits or are the limits shared with other coverages (management liability, employment liability, professional liability)?
• Size and location of the insured and its customers.
• Customer profile.
Key Takeaways

• Know your insurance program.
• Know your limits.
• Review policy and limits annually.
• Know how to report a claim.
• Know how to interact with the insurance company.
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.
Risk Shifting By Agreements With Vendors, Others

Cyber Insurance EG’s:

“The Provider shall maintain insurance for all claims, suits, actions, liabilities, damages, losses, costs and expenses (including attorney’s fees) of any nature to which the Company may be subjected [as a result from / in any way involving] the Provider’s access to, use, handling, storage, transmission, or disposal of any data/information (including paper records), ...”

OR

“... SERVICE PROVIDER shall, at its own expense, procure [Policy Name, eg Software Professional Liability E&O Insurance], or such other insurance as is necessary to ensure coverage for any and all acts, omissions, errors of SERVICE PROVIDER with respect to Services performed and materials provided under this Agreement, including but not limited to: [Liability coverage type and minimum required policy limits per claim / aggregate]”

Potential Issues Include:
Two Contracts (Agreement and Insurance Policy) to enforce, interpret and reconcile; or Silent Contracts
Emerging Issues – What’s Next?

- Current court cases involve traditional data breaches
- Smart, data centric technology is entering into nearly all facets of daily life
- How will insurance products deal with this new reality?
- Relatively New Areas To Consider:
  1 – Internet of Things ("I-o-T")
  2 – Biometrics
  3 – Artificial and Virtual Intelligence
Pre-Breach Preparedness

I. Your Security Posture: Privacy Risk Assessment

- What type of information do you process, transmit or store?
- Where is it stored?
- How is it protected?
- How long do you retain it?

- Inventory and track equipment
- Update and patch software
- Control and log access to data
- Segment networks and minimize data
II. 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
III. Planning to Respond

- Develop a tailored, written plan that identifies your response team and their jobs
- Identify the resources needed to implement
- Test
- Update
• Organizations must recognize and respond to indicators of compromise

  – Disabling of controls like firewalls, anti-virus, etc.
  – Administrator activity outside the IT sub-network.
  – Use of previously inactive accounts.
  – Installation of new hardware or software.
  – Password guessing.
  – Unusual file transfers.
V. Risk Management

Essential Components Are:

- People
- Processes
- Technology
Preparation for a Breach: Cyber Insurance

- Your CGL policy does not cover data loss or “cyber” events ...
- What does your policy cover?
  - First party losses and costs?
  - Third party costs?
  - Remediation costs?
  - Fines and penalties?
  - Risk management services?
  - Selection of outside counsel?
  - Selection of breach responders?
  - Employee owned devices?
  - What is the retroactive date?
- Do the limits of liability match your realistic exposure?
Challenges to Anticipate

- People
- Processes
- Technology
Questions & Answers

Panel

- Amelia Gerlicher, Perkins Coie LLP
  206.359.3445 | agerlicher@perkinscoie.com

- Jason Glasgow, Travelers Insurance
  860.277.4231 | jglasgow@travelers.com

- Tom Schauer, CliftonLarsonAllen
  253 468 9750 | tom.schauer@claconnect.com

- Timothy Wallach, Supervisory Special Agent, Cyber Task Force, FBI
  206.287.3601 | Timothy.Wallach@ic.fbi.gov

Moderator
Michael Handler, Esq., Cozen O’Connor
206.808.7839 | mhandler@cozen.com