CYBER LIABILITY SYMPOSIUM
Panel

• Patrick Clabby, AVP Underwriting, Ace North America
• Sean Hoar, Esq., Davis Wright Tremaine
• Timothy Wallach, Supervisory Special Agent, Cyber Task Force, FBI Seattle Division
• Brent Williams-Ruth, Esq., Scheer & Zehnder

Moderator

• Peter Marchel, Esq., Marchel & Associates Risk Consulting
STATISTICS & TRENDS

• How compromises are being detected.
• Length of time to discover compromise.
• Reasons for the lag time.
WHAT ARE THE NUMBERS?

• Mandiant’s Mtrends 2015: A View From the Front Lines
  – Compromise detection victims notified by external entity 69%.
  – 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
**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>
WHAT ARE THE NUMBERS?

• Ponemon Institute (2014):
  – $5.85M – Avg. cost per data breach
  – $201 (USD) – Avg. cost per record
  – $8.9M – Avg. annualized cost of U.S. cybercrime
  – 102 – Avg. successful attacks on organizations per week

• Causes of Compromise:
  – 44% – malicious/criminal attacks
    • $246 avg. cost per record
  – 31% – negligence/human factors
    • $160 avg. cost per record
  – 25% – system glitches
    • $171 avg. cost per record

• Note: Ponemon excludes breaches exceeding 100k records from its analysis. Breach range for 2014 was 5,000 to 100,000 records
THREAT LANDSCAPES

• Different threats can implicate different insurance policies
Risk Factors

First Party & Third Party
- Crime / EE Theft
- Beneficiaries

Employee / Other
- Commercial General Liability

Cyber
- Entity

Management

Errors & Omissions
- Regulatory / Stakeholder

Employment
- Employee / Regulatory

Lending / Other

Fiduciary / Benefits
- 9
Where are the threats?

• **Inside threats**
  – Employee negligence
    • Security failures
    • Lost mobile devices
  – Employee ignorance
    • Improper disposal of personal information (dumpsters)
    • Lack of education and awareness
  – Malicious employees

• **Outside threats**
  – Hackers
    • Malware
    • Phishing and Spear Phishing
  – Thieves (including Social Engineering Tools)
  – Vendors
Across the Cyber Threat Landscape
Cyber threat actors are exploiting networks for an ever-widening array of economic and political objectives.

<table>
<thead>
<tr>
<th>Objective</th>
<th>NUISANCE</th>
<th>DATA THEFT</th>
<th>CYBER CRIME</th>
<th>HACKTIVISM</th>
<th>DESTRUCTIVE ATTACK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td>Botnets &amp; Spam</td>
<td>Advanced Persistent Threat Groups</td>
<td>Credit Card Theft</td>
<td>Website Defacements</td>
<td>Delete Data</td>
</tr>
<tr>
<td>Targeted Character</td>
<td>Often Automated</td>
<td>Persistent</td>
<td>Frequently Opportunistic</td>
<td>Conspicuous</td>
<td>Conflict Driven</td>
</tr>
</tbody>
</table>

Mandiant’s Mtrends 2015: A View From the Front Lines
### All Sectors are Vulnerable

#### 2015 Verizon Data Breach Investigations Report

<table>
<thead>
<tr>
<th>INDUSTRY</th>
<th>TOTAL</th>
<th>SMALL</th>
<th>LARGE</th>
<th>UNKNOWN</th>
<th>TOTAL</th>
<th>SMALL</th>
<th>LARGE</th>
<th>UNKNOWN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accommodation (72)</td>
<td>368</td>
<td>181</td>
<td>90</td>
<td>97</td>
<td>223</td>
<td>180</td>
<td>10</td>
<td>33</td>
</tr>
<tr>
<td>Administrative (56)</td>
<td>205</td>
<td>11</td>
<td>13</td>
<td>181</td>
<td>27</td>
<td>6</td>
<td>4</td>
<td>17</td>
</tr>
<tr>
<td>Agriculture (11)</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Construction (23)</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Educational (61)</td>
<td>165</td>
<td>18</td>
<td>17</td>
<td>130</td>
<td>65</td>
<td>11</td>
<td>10</td>
<td>44</td>
</tr>
<tr>
<td>Entertainment (71)</td>
<td>27</td>
<td>17</td>
<td>0</td>
<td>10</td>
<td>23</td>
<td>16</td>
<td>0</td>
<td>7</td>
</tr>
<tr>
<td>Financial Services (52)</td>
<td>642</td>
<td>44</td>
<td>177</td>
<td>421</td>
<td>277</td>
<td>33</td>
<td>136</td>
<td>108</td>
</tr>
<tr>
<td>Healthcare (62)</td>
<td>234</td>
<td>51</td>
<td>38</td>
<td>145</td>
<td>141</td>
<td>31</td>
<td>25</td>
<td>85</td>
</tr>
<tr>
<td>Information (51)</td>
<td>1,496</td>
<td>36</td>
<td>34</td>
<td>1,426</td>
<td>95</td>
<td>13</td>
<td>17</td>
<td>65</td>
</tr>
<tr>
<td>Management (55)</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Manufacturing (31–33)</td>
<td>525</td>
<td>18</td>
<td>43</td>
<td>464</td>
<td>235</td>
<td>11</td>
<td>10</td>
<td>214</td>
</tr>
<tr>
<td>Mining (21)</td>
<td>22</td>
<td>1</td>
<td>12</td>
<td>9</td>
<td>17</td>
<td>0</td>
<td>11</td>
<td>6</td>
</tr>
<tr>
<td>Other Services (81)</td>
<td>263</td>
<td>12</td>
<td>2</td>
<td>249</td>
<td>28</td>
<td>8</td>
<td>2</td>
<td>18</td>
</tr>
<tr>
<td>Professional (54)</td>
<td>347</td>
<td>27</td>
<td>11</td>
<td>309</td>
<td>146</td>
<td>14</td>
<td>6</td>
<td>126</td>
</tr>
<tr>
<td>Public (92)</td>
<td>50,315</td>
<td>19</td>
<td>49,596</td>
<td>700</td>
<td>303</td>
<td>6</td>
<td>241</td>
<td>56</td>
</tr>
<tr>
<td>Real Estate (53)</td>
<td>14</td>
<td>2</td>
<td>1</td>
<td>11</td>
<td>10</td>
<td>1</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>Retail (44–45)</td>
<td>523</td>
<td>99</td>
<td>30</td>
<td>394</td>
<td>164</td>
<td>95</td>
<td>21</td>
<td>48</td>
</tr>
<tr>
<td>Trade (42)</td>
<td>14</td>
<td>10</td>
<td>1</td>
<td>3</td>
<td>6</td>
<td>4</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Transportation (48–49)</td>
<td>44</td>
<td>2</td>
<td>9</td>
<td>33</td>
<td>22</td>
<td>2</td>
<td>6</td>
<td>14</td>
</tr>
<tr>
<td>Utilities (22)</td>
<td>73</td>
<td>1</td>
<td>2</td>
<td>70</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>Unknown</td>
<td>24,504</td>
<td>144</td>
<td>1</td>
<td>24,359</td>
<td>325</td>
<td>141</td>
<td>1</td>
<td>183</td>
</tr>
</tbody>
</table>

**TOTAL**                  | 79,790| 694   | 50,081| 29,015  | 2,122 | 573   | 502   | 1,047   |
# Types of Attack Per Sector

<table>
<thead>
<tr>
<th>Sector</th>
<th>Crime &amp; Espionage</th>
<th>Denial of Service</th>
<th>Lost/Stolen Assets</th>
<th>Miscellaneous Errors</th>
<th>Payment Card/Smashers</th>
<th>Point of Sale</th>
<th>Privilege Misuse</th>
<th>Web Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCOMMODATION</td>
<td>1%</td>
<td>9%</td>
<td>1%</td>
<td>2%</td>
<td>91%</td>
<td>5%</td>
<td>1%</td>
<td></td>
</tr>
<tr>
<td>ADMINISTRATIVE</td>
<td>32%</td>
<td>15%</td>
<td>11%</td>
<td>26%</td>
<td>73%</td>
<td>45%</td>
<td>18%</td>
<td></td>
</tr>
<tr>
<td>EDUCATIONAL</td>
<td>36%</td>
<td>2%</td>
<td>7%</td>
<td>14%</td>
<td>12%</td>
<td>11%</td>
<td>31%</td>
<td></td>
</tr>
<tr>
<td>ENTERTAINMENT</td>
<td>1%</td>
<td>16%</td>
<td>32%</td>
<td>1%</td>
<td>2%</td>
<td>7%</td>
<td>9%</td>
<td></td>
</tr>
<tr>
<td>FINANCIAL SERVICES</td>
<td>14%</td>
<td>37%</td>
<td>2%</td>
<td>5%</td>
<td>11%</td>
<td>7%</td>
<td>35%</td>
<td></td>
</tr>
<tr>
<td>HEALTHCARE</td>
<td>34%</td>
<td>60%</td>
<td>25%</td>
<td>17%</td>
<td>8%</td>
<td>33%</td>
<td>1%</td>
<td></td>
</tr>
<tr>
<td>INFORMATION</td>
<td>8%</td>
<td>25%</td>
<td>2%</td>
<td>10%</td>
<td>5%</td>
<td>4%</td>
<td>4%</td>
<td></td>
</tr>
<tr>
<td>MANUFACTURING</td>
<td>25%</td>
<td>52%</td>
<td>5%</td>
<td>3%</td>
<td>23%</td>
<td>11%</td>
<td>6%</td>
<td></td>
</tr>
<tr>
<td>MINING</td>
<td>51%</td>
<td>5%</td>
<td>3%</td>
<td>10%</td>
<td>4%</td>
<td>5%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OTHER SERVICES</td>
<td>11%</td>
<td>10%</td>
<td>70%</td>
<td>3%</td>
<td>5%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PUBLIC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROFESSIONAL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>professional</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PUBLIC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RETAIL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2015 Verizon Data Breach Investigations Report
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
Types of Data Breach Costs

- First-party:
  - **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**;
Types of Data Breach Costs

• First-party:
  – cyber extortion:
    • payment to criminals that have installed “ransomware” on a system and proceeded to encrypt everything connected to the point of entry for the ransomware – 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 the various data breach notification statutes or regulatory schemes;
  – other crime loss which may involving the following costs:
    • money lost through computer fraud or funds transfer fraud – which may happen when a hacker infiltrates a network and uses a combination of social engineering and technical subterfuge to steal money.
Types of Data Breach Costs

- **Third-party** losses/costs to customers and governmental entities:
  - media liability (including copyright and trademark infringement);
  - privacy liability to employees or customers for breach of privacy;
  - bodily injury – which is an increasing concern in the healthcare environment should the wrong medication be dispensed, or a linked implant go awry;
  - defensive litigation:
    - class actions;
    - derivative actions; and
    - regulatory actions.
Types of Data Breach Costs

- **Remediation costs:**
  - legal services which will involving drafting of consumer and regulatory notification letters;
  - forensics services which will include imaging of devices, scanning for malware, analysis of data, review of log files, etc.;
  - crisis management services, including public relations expenses beyond consumer notification (these typically occur in high-profile breaches, or with high-profile clients ...);
  - consumer and regulatory notification – the actual hard copy costs if notification is not sent electronically,
  - call center services - depending upon the scale of the breach;
  - credit monitoring and identity theft protection services – historically obtained for approximately $17.60 per consumer, although the wholesale market is driving that cost down a bit.
Types of Data Breach Costs

• **Fines and penalties:**
  – expenses of regulatory investigations;
  – civil judgments;
  – fines and penalties levied by regulatory authorities; and
  – fines and penalties for payment card industry compliance violations.
EVOLVING THREAT TRENDS

- Breach from External Threat  (80%)
- Phishing 23%, 11% open attachments
- Spyware/Keylogger 5%
- Ram Scrapper  20% (largest increase)
- Credentials 52%

Verizon 2015 Data Breach Investigations Report
AVERAGE NUMBER OF MALWARE EVENTS PER WEEK FOR 5 INDUSTRIES:

- Financial Services (350)
- Insurance (575)
- Retail (801)
- Energy/Utilities (772)
- Education (2,332)

Verizon 2015 Data Breach Investigations Report
LEGAL LANDSCAPE
LEGISLATING THE ISSUE

- **Federal Government** – 5+ major statutory schemes
- **State Laws** – At least 46 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**...

WHO IS MAKING THE DECISIONS?

- Likely will be in Federal Court (lifetime appointment)

- More specifically, “Judges” typically =
  - Not social media wizards
  - Difficulty using internet (“interwhat?”)
  - “Text” means words on paper
  - 10 e-mails in a day is “a lot”
  ...you get the idea
STANDING: WHO CAN SUE?

- No clear answer….Split among the Circuits

- Increased Risk of Injury Is Sufficient (i.e. no proven damages)
  - Krottner v. Starbucks Corp. (9th Cir. 2010) (laptop with personally identifiable information stolen)
  - Pisciotta v. Old Nat’l Bancorp (7th Cir. 2007) (data breach by hacker)

- Increased Risk Not Enough, Future Damages Must Be “Certainly Impending” (or must have actual damages)
  - Reilly v. Ceridian Corp (3rd Cir. 2011) (data breach did not result in actual misuse of personal information)
STANDING DOES NOT MEAN LIABILITY

**Krottner v. Starbucks Corp.**, 628 F.3d 1139 (9th Cir. 2010)

Court found standing but...case was dismissed because no evidence that the information had been misused, and therefore there was **no harm or “injury in fact.”**
THE DAMAGES TO THE BUSINESS

- MULTIPLE AVENUES OF FINANCIAL LOSS TO BUSINESS
  - Regulatory Fines
  - Litigation (Government and Private actions, Class Action)
  - Loss of Reputation = Lost Customers
  - Loss of Productivity
  - Loss of System Availability
  - Loss of Intellectual Property

- LOSS OF REPUTATION FROM MULTIPLE SOURCES
  - Required public notice to involved consumers
  - Press and internet (blogs, et al.)
  - Government (Attorneys General...etc.)
THE CONSUMER’S DAMAGES: A VERY LOW BAR

- **Claridge v. RockYou Inc.**, 785 F. Supp. 2d 855 (N.D. Cal. 2011)
  - RockYou is **publisher/developer of online services** and apps for use with Facebook, MySpace...etc.

  - Customer sued RockYou alleging it **failed to secure its users' sensitive personally identifiable information** (“PII”) (i.e. e-mail address, password, login credentials)

  - Plaintiff alleged he **lost an ascertainable but unidentified “value” and/or property right** inherent in the PII.

  - **Court agreed that PII has value** and refused to dismiss breach of contract and negligence claims
COVERAGE UNDER CGL POLICIES

- 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 duty to defend Eyeblaster, Eyeblaster files declaratory judgment action...
Software explicitly excluded, but computer is tangible property and it could no longer function, thereby meeting definition of “property damage”

- **Note:** Plaintiff’s computer ruled to not be “impaired property” because no evidence computer could be restored to use after removing Eyeblaster software – Court appeared to be ignorant of fact that computer can be fully wiped. (Old judge problem?)
PERSONAL AND ADVERTISING INJURY

- Coverage B of traditional CGL provides coverage for “personal and advertising injury”

- Defined, in part, as injury arising out of oral/written publication, in any manner, of material that violates person’s right of privacy
  - What is “publication”???

- **Four Privacy Claims:**
  - Publicity to Private Life (the right to secrecy)
  - Appropriation of Name or Likeness
  - Placing Someone in a False Light
  - Intrusion upon Seclusion (the right to be left alone)
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.”
LATEST COURT DECISIONS OBSOLETE?

- Courts are slow, lagging way behind

- New Products largely untested in courts...

- ...and New Exclusions coming for CGL policies:
  - Close the window of unintended potential coverage for both Coverage A and Coverage B
  - More than 40 states have already approved of the new exclusions
  - Effective as of May 2014
COMMONALITIES OF BREACH AND RESPONSE TO BREACH

• Different threats can implicate different insurance policies
Data Breach Life Cycle

Access the Problem
- Discover breach
- Contain losses, secure area
- Alert preparedness team
- Notify law enforcement
- Notify regulators

Engage External Resources
- Alert vendor
- Call forensics team
- Alert public relations (internal or external)

Comply with Notification
- Draft and send notification
- Active call center
- Public disclosure (if appropriate)

Manage Ongoing Business
- Continue assuring customers
- Continue data systems monitoring
- Resume business as usual
Mitigating Cyber Expenses

• Questions to Ask About Insurance:
  – What are the right limits?
  – How do I pick the right coverage / company?
  – What happens when a claim occurs?
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.
PUTTING CYBER POLICY RESOURCES TO WORK FOR THE INSURED

• Access the problem
• Engage external resources
• Comply with notification
• Managing ongoing business
Cyber Coverage = Access to Resources

- Notification Services
- Forensics
- Legal Services
- Breach Coach

www.marchelassociates.com | proprietary & confidential
Factors that decrease the cost of a data breach

- Strong security posture
- Incident response planning
- Business continuity management
- CISO appointment

Factors that increase the cost of a data breach

- Lost or stolen devices
- Third party involvement
- Notification before investigation completed

Source: 2014 Cost of Data Breach Study: Global Analysis
Sponsored by IBM, Conducted by Ponemon Institute LLC
Information Security Incident Cycle

- Preparation
- Detection & Analysis
- Containment Eradication & Recovery
- Post-Incident Activity

How Do You Increase Security?

**Conduct inventory of data**

<table>
<thead>
<tr>
<th>Preparation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What type of information do you process, transmit or store?</strong></td>
</tr>
<tr>
<td>- Personally identifiable information (PII)</td>
</tr>
<tr>
<td>- Protected health information (PHI)</td>
</tr>
<tr>
<td>- Payment Card Industry (PCI) information</td>
</tr>
<tr>
<td>- Corporate confidential information</td>
</tr>
<tr>
<td>- Employee information</td>
</tr>
</tbody>
</table>

| Where is the information stored? |
| - Servers/devices onsite? |
| - Services in the cloud? |

| How is the information protected? |
| - Is data encrypted? |
| - Who has access? |

| How long do you retain the information? |
| - Do you have a data retention policy? |
How Do You Increase Security?

Implement best practices

- Conduct inventory of all hardware and software
- Use current version of operating systems
- Automate security patching
- Enable intrusion detection and prevention systems
- Segment network
- Control access based on need to know
- Use multi-factor authentication

- Eliminate unnecessary data and processes
- Protect data
- Monitor endpoints
- Conduct due diligence on all third party service providers
- Conduct risk assessments
- Conduct vulnerability testing
- Develop incident response plan
- Test incident response plan with “tabletop” exercises
How Do You Increase Security?

Develop Incident Response Plan

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Key Team Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Improve information security</td>
<td>▪ CISO/IT Lead</td>
</tr>
<tr>
<td>▪ Prepare efficient, effective response to</td>
<td>▪ Legal/Outside counsel</td>
</tr>
<tr>
<td>information security incident</td>
<td>▪ Financial management</td>
</tr>
<tr>
<td>▪ Systematic</td>
<td>▪ Risk management</td>
</tr>
<tr>
<td>▪ Minimal loss or theft</td>
<td>▪ Human resources</td>
</tr>
<tr>
<td>▪ Minimal disruption</td>
<td>▪ Breach response vendors</td>
</tr>
<tr>
<td>▪ Legally compliant</td>
<td>▪ Outside counsel</td>
</tr>
<tr>
<td>▪ Preserve reputation</td>
<td>▪ Forensics</td>
</tr>
<tr>
<td>▪ Collect evidence of attack</td>
<td>▪ Notification</td>
</tr>
<tr>
<td>▪ Coordinate remediation</td>
<td>▪ Call center</td>
</tr>
<tr>
<td>▪ Recover and restore</td>
<td>▪ Credit monitoring</td>
</tr>
<tr>
<td>information system</td>
<td>▪ Identity restoration</td>
</tr>
<tr>
<td></td>
<td>▪ Public relations/crisis</td>
</tr>
<tr>
<td></td>
<td>communications</td>
</tr>
</tbody>
</table>
### Establish Incident Response Team

<table>
<thead>
<tr>
<th>Outside Counsel</th>
<th>Breach Response Vendors</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Project management skill</td>
<td>▪ MSAs in place</td>
</tr>
<tr>
<td>▪ Crisis management skill</td>
<td>▪ Fewer decisions during digital crisis</td>
</tr>
<tr>
<td>▪ Breach response experience</td>
<td>▪ Reduced costs</td>
</tr>
<tr>
<td></td>
<td>▪ Instant response</td>
</tr>
<tr>
<td></td>
<td>▪ Existing relationship</td>
</tr>
<tr>
<td></td>
<td>▪ Knowledge of network</td>
</tr>
<tr>
<td></td>
<td>▪ Knowledge of breach notification requirements</td>
</tr>
<tr>
<td></td>
<td>▪ Knowledge of privacy and security law</td>
</tr>
<tr>
<td></td>
<td>▪ Existing relationship</td>
</tr>
<tr>
<td></td>
<td>▪ Knowledge of vulnerability test data</td>
</tr>
<tr>
<td></td>
<td>▪ Engagement in place</td>
</tr>
<tr>
<td></td>
<td>▪ Table top exercise partner</td>
</tr>
<tr>
<td></td>
<td>▪ Trusted partner</td>
</tr>
<tr>
<td></td>
<td>▪ Knowledge of business</td>
</tr>
<tr>
<td></td>
<td>▪ Attorney/client privilege</td>
</tr>
</tbody>
</table>
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?
The Initial Response to a Breach

- Conduct an assessment with CISO/IT Lead
  - If possible breach - implement incident response plan
- Notify insurer
  - Confirm approval of all breach response vendors
- Engage outside counsel
- Engage digital forensics team through outside counsel
- Implement litigation hold
- Begin to assess whether additional breach response vendors may be necessary
  - Public relations/crisis communications
  - Notification
  - Call center
  - Remediation services
Containment/Eradication/Recovery

- Deploy forensics firm to assess, contain, eradicate, analyze and remediate
  - Identify target of breach, i.e. PII, PHI, IP, PCI data, financial account information, etc.
  - Determine whether data loss occurred; if so, whether it has stopped
  - Eliminate threat
  - Determine extent of loss
- Preserve and secure evidence, including all log files
- Recovery – return affected systems to normal operations
Post-incident Activity

- Determine whether to notify law enforcement
- Determine whether breach notification is required
  - If law enforcement is notified, and if breach notification is required, determine whether notification should be delayed pending law enforcement investigation
- If breach notification is required
  - Determine whether remediation services will be provided
  - Draft notification letters and frequently asked questions
  - Send notification letters to affected consumers and regulatory officials
- Prepare for post-incident regulatory response
- Conduct post-incident debrief
<table>
<thead>
<tr>
<th>Exposure Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Security Liability</td>
<td>Provides liability coverage if an Insured’s Computer System fails to prevent a Security Breach or a Privacy Breach</td>
</tr>
<tr>
<td>Privacy Liability</td>
<td>Provides liability coverage if an Insured fails to protect electronic or non-electronic information in their care, custody, and control</td>
</tr>
<tr>
<td>Media Liability</td>
<td>Covers the Insured for Intellectual Property and Personal Injury perils that result from an error or omission in content (coverage for Patent and Trade Secret are generally not provided)</td>
</tr>
<tr>
<td>Regulatory Liability</td>
<td>Coverage for lawsuits or investigations by Federal, State, or Foreign regulators relating to Privacy Laws</td>
</tr>
<tr>
<td>Crisis Management</td>
<td></td>
</tr>
<tr>
<td>Notification Expense</td>
<td>1st Party expenses to comply with Privacy Law notification requirements</td>
</tr>
<tr>
<td>Credit Monitoring Expense</td>
<td>1st Party expenses to provide up to 12 months credit monitoring</td>
</tr>
<tr>
<td>Forensic Investigations</td>
<td>1st Party expenses to investigate a system intrusion into an Insured Computer system</td>
</tr>
<tr>
<td>Public Relations</td>
<td>1st Party expenses to hire a Public Relations firm</td>
</tr>
<tr>
<td>Data Recovery</td>
<td>1st Party expenses to recover data damaged on an Insured Computer System as a result of a Failure of Security</td>
</tr>
<tr>
<td>Business Interruption</td>
<td>1st Party expenses for lost income from an interruption to an Insured Computer System as a result of a Failure of Security</td>
</tr>
<tr>
<td>Cyber Extortion</td>
<td>Payments made to a party threatening to attack an Insured’s Computer System in order to avert a cyber attack</td>
</tr>
<tr>
<td>Technology Services/Products &amp; Professional Errors &amp; Omission Liability</td>
<td>Technology Products &amp; Services and Miscellaneous E&amp;O can be added to a policy when applicable</td>
</tr>
</tbody>
</table>
NEW EXCLUSION – DISCLOSURE OF DATA

- Coverage A: New exclusion reads in part...

“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.”
NEW EXCLUSION – DISCLOSURE OF DATA

- Coverage B: New 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.**”
HOLES IN 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.
NEW LIABILITIES NOT ANTICIPATED

- The evolution of cyber liability claims has a familiar ring to it.

- Insurers have been through this before with toxic torts – “pollution”

- Cyber liability claims have emerged out of the advancement of industry through new technology
  - Result is the amendment of the CGL policy and creation of new insurance products

- But are insurers moving fast enough, thinking outside the box, and imagining the future risks?
SO 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?
- Three Relatively New Areas To Consider:
  1. **Internet of Things ("I-o-T")**
  2. **Bring Your Own Device ("BYOD")**
  3. **Cloud Computing**
NEW RISK: I-O-T

EXAMPLES:

- Medical Devices

- Baby Monitor in special pj’s
  - Body positioning, breathe rate, heart rate – help prevent SIDS

- Smart Thermostats for your home (Nest)

- Municipal Garbage Cans
  - Alerts when a bin needs to be emptied

- Manufacturing Maintenance and Repairs
  - Sensors installed inside equipment will monitor if any parts have exceeded their designed thresholds
WHAT ARE THE RISKS WITH I-O-T?

- The Shared Common Trait of I-o-T: Device receives information that is then transmitted to another device
  - What if the I-o-T **device malfunctions**?
  - What if the **data/software compromised**?
  - What if **data corrupted** going to/from device?
  - Is I-o-T a product? A service? **Both**?
  - What if there is **human error** at monitoring station?
- What types of insurance cover these risks, and would any of these fall under a traditional CGL?
EXAMPLE FOR YOUR CONSIDERATION

- I-o-T Pacemaker for the heart (coming soon)

- Monitoring station receives data from pacemaker, looking at functionality, battery, potential maintenance/repair/replacement

- Monitoring station transmits information to pacemaker to maintain optimal functionality of device

- Will your Cyber insurance product consider all the avenues of risk with this product/service?
  - Catastrophic Damages – Death or Brain Damage
  - What if system hacked and ALL customers affected?

- HOW CLOSE ARE WE TO THE FOREGOING?: Recently it was revealed there was a security concern regarding someone “hacking” into former U.S. Vice President Dick Cheney’s pacemaker.
LET’S CONSIDER BYOD

- **Bring-Your-Own-Device (“BYOD”)** technologies are the new popular and cost-effective means of providing mobility and flexibility to employees via employee owned and controlled devices.

- **Plethora of risks created because BYOD devices are:**
  - Owned and controlled by employees;
  - Who have uncertain means of securing/controlling device;
  - Who employer is trusting to maintain security;
  - Who employer is trusting to be honest/loyal;
  - The device is connected and interacting directly with the IT system (i.e. not an isolated website with firewalls);
  - Employer has (probably) limited idea what employee is doing, particularly outside of work.
WHAT THESE BYOD RISKS MEAN

- Risk of **inadvertent damage** to system: viruses, et. al.
- Control of **access** rights – how?
- Risk of being **hacked**: compromised data, viruses, et al.
  - Risks to customers and other employees
- Tracking/**Monitoring employees**:
  - Employee privacy? How far should/can employer go?
- Remote **wiping** of company info on employee’s device?
  - Accidental wiping of employee personal info.
- Does the employer have good rights agreement with employee? i.e. **employer** rights broad, **employee** rights ltd.+ waiver of liability
- BYOD also implicates Employment Liability insurance. Are you factoring BYOD into your underwriting of such policies?
“CLOUD” COMPUTING RISKS/ISSUES

- “Cloud Computing” = Delivering hosted services over the internet. Three Categories:
  1 – Infrastructure (i.e. your server and storage is hosted offsite)
  2 – Platform (i.e. software/product development tools hosted – apps)
  3 – Software (i.e. runs the apps that are on the platform)

- Worldwide spending on cloud computing $42 billion in 2013

- Do your Cyber policies consider the scope of risk? Few Issues:
  - Location of host? Does it matter?
  - How is location determined? Corporate office? Location of data?
  - What is the “coverage territory”?
  - Where did data breach occur? How do you determine?
  - Does it matter? Jurisdiction?
When determining the risk you intend to insure, you need to know how long you may be on the risk.

Statute of Limitations (“SOL”) must be part of that assessment, but what is the SOL for plaintiffs?

When is “discovery” – i.e. When discover the data compromised? When damages discovered/occurred?

Courts have not decided the SOL question.

Another Issue: Claims made vs. Occurrence policy?
  - Continuous trigger?
At this point, one thing is clear: **Technology is changing faster than policy provisions**

- Remember the audience: U.S. judges and juries
- Courts generally construe ambiguity against insurer
- Specific terminology, even if understood, may be obsolete by the time it makes it into a policy
- Is your language understood by the common man/woman in the U.S.?

**Consider Terminology Used in Policies:**
- “Trojan Horse,” “Worm,” “Smurf Attack,” “Logic Bomb”
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.
Key Takeaways (cont.)

• Every system is vulnerable.
• Bad guys are:
  – Persistent
  – Well-resourced
  – Increasingly sophisticated
• Increase your security system.
• Prepare for the inevitable incident.
Key Takeaways (cont.)

• Understand your exposure
  – Number and type of records
• Understand where data resides
  – Who has access
• Understand liability falls with the owner of the data
• Establish relationships externally or internally to prepare for pre and post breach
Key Takeaways (cont.)

• Know your insurance program
  – Do you have a cyber specific policy?
• Know your exposures.
Question & Answer

Panel
Patrick Clabby, AVP Underwriting, Ace North America
T:(415)547-4433   E:patrick.clabby@acegroup.com

Sean Hoar, Esq., Davis Wright Tremaine
T:(206) 622-3150   E:seanhoar@dwt.com

Brent William-Ruth, Esq., Scheer & Zehnder
T:(206) 262-1200   E:bwilliams-ruth@scheerlaw.com

Timothy Wallach, Supervisory Special Agent, Cyber Task Force, FBI Seattle Division
1110 3rd Avenue, Seattle, WA 98101

Moderator
Peter Marchel, Esq., Marchel & Associates Risk Consulting
T:(425) 788-4349   E:peterm@marchelassociates.com