Cyber Risk-Transfer and Incident Response

You’ve been breached – what happens next?

Wayne Dean – McGriff Insurance Services
Hannah Hoeflinger - INSUREtrust
Welcome

Today we want to discuss some of the things that we do in our day-to-day operations with regards to coverage analysis, market trends, claims, incident response plans and how they relate to your business and your industry.

We would like for this to be an open forum for you to ask any questions you might have about your Risk Management Program, in particular your Cyber coverage.

Please ask questions! We welcome the dialogue.
Who We Are

- **McGriff Insurance Services** is the 5th largest insurance brokerage in the US
  - Preferred Business Solutions Partner for PSA Corporate and it’s members for 5 years
  - Work as a consultative partner with many PSA members on Risk Management programs
  - Dedicated to helping reduce our clients cost, improve our clients productivity, EBITDA, and ownership valuation. Our primary focus is Commercial Property, General liability, Commercial Auto, Workers Compensation, Commercial Umbrella, Professional liability (CYBER, E & O, Fiduciary, and D & O), Life Insurance, and Bonding needs
INSUREtrust is our partner broker for Cyber and Professional lines and is a cyber and technology specialist broker headquartered out of Atlanta, Georgia.

- Cyber Industry Pioneers – 1997
- Recognized as largest cyber wholesaler for Axis, Beazley, CFC, and more
- In the last 4 years, INSUREtrust has seen growth in excess of 30% year over year.
- 2017 and 2019 Advisen Cyber Risk Broking Team of the Year
The Risk Transfer Conversation

- How are you all having the conversation around Cyber or Technology risk right now? What common pushbacks do you see when it comes to transferring that risk to a Cyber Insurance Policy?
State Of The Cyber Market

- Total impact of cyber crime in 2018 was over $400 Billion
- Over 45% of SMBs are required to buy cyber insurance to comply with customer contracts
- A new organization will fall victim to ransomware every 14 seconds in 2019, and every 11 seconds by 2021. (Source: Cyber Security Ventures)
- 1.5 million new phishing sites are created every month and ransomware attacks coming from phishing emails increased 109 percent from 2017 to 2019. (Source: webroot.com and PhishMe)
- Ransomware attacks have increased over 97 percent in the past two years. (Source: PhishMe)
Cyber Insurance 2019

- Race to keep up with sophisticated hacking activity
- IOT and race for innovative technology = race for innovative coverage
- 170 carriers with varying experience: 30 more than 5 years – 10 more than 10 years
- Cyber first carriers growing in premium by 25% a year
What are common Cyber Risks?

Average Losses In 2018

Average cost of a breach overall:

$604,000

Average cost of a breach broken out into first party averages:

- Crisis Services: $307,000
- Legal Defense: $106,000
- Legal Settlement: $224,000
What are common Cyber Risks?
Average Losses In 2018

Average cost of a phishing event: $93,000
Average cost of a ransomware attack: $229,000
Average cost of a Business Interruption loss: $2,000,000
Leading Threats to Data

- Employee Mistakes
- Hackers
- System of Process Malfunction
- Malicious Insiders
- Temporary or Contract Workers
- Third-party Service Providers
- Lawful Data Request (i.e. by Gov. Authorities)
## Types of Threats and Impacts

<table>
<thead>
<tr>
<th>Motives</th>
<th>Targets</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Nation state</strong></td>
<td><strong>Organised crime</strong></td>
<td><strong>Hacktivists</strong></td>
</tr>
<tr>
<td>• Economical or political advantage</td>
<td>• Immediate financial gain</td>
<td>• Influence political and/or social change</td>
</tr>
<tr>
<td><strong>Insiders</strong></td>
<td>• Collect information for future financial gains</td>
<td>• Pressure business to change their practices</td>
</tr>
<tr>
<td>• Trade secrets</td>
<td>• Financial/payment systems</td>
<td>• Corporate secrets</td>
</tr>
<tr>
<td>• M&amp;A information</td>
<td>• Personally identifiable or sensitive information</td>
<td>• Sensitive business information</td>
</tr>
<tr>
<td>• Critical financial systems and information</td>
<td>• Payment card information</td>
<td>• Critical financial systems</td>
</tr>
<tr>
<td></td>
<td>• Protected health info</td>
<td>• Personally identifiable/sensitive information</td>
</tr>
<tr>
<td></td>
<td><strong>Impact</strong></td>
<td><strong>Insiders</strong></td>
</tr>
<tr>
<td>• Loss of competitive advantage</td>
<td>• Regulatory investigation/penalty</td>
<td>• Personal advantage</td>
</tr>
<tr>
<td>• Regulatory investigation/penalty</td>
<td>• Law suits</td>
<td>• Monetary gain</td>
</tr>
<tr>
<td>• Disruption to critical infrastructure</td>
<td>• Brand and reputation</td>
<td>• Professional revenge</td>
</tr>
<tr>
<td></td>
<td>• Loss of consumer confidence</td>
<td>• Bribery or coercion</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Administrative credentials</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Trade secret disclosure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Operational disruption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Loss of consumer confidence</td>
</tr>
</tbody>
</table>
Why Do I Need a full Cyber Insurance policy?

- Operations and Contractual Requirements
- Weak coverage on GL policy

What am I getting for my money?

- Cyber insurance provides a great deal of value other than just loss of data coverage
  - Driving cost of a breach down with expert vendors
  - Pre and Post Breach resources
  - Vulnerability reports
  - Up-front claims assistance
Do I Have Any Cyber Coverage?

- Who here has Cyber Insurance?
  - Separate Cyber Policy or Included in GL policy

- Who has had a Cyber incident? What happened?
  - Incident Response Plan
What Is Covered?

- Basics include: Privacy Liability, Network Security, Electronic Data, Breach of Privacy
- Additional Coverage Considerations: Notification Costs (inside limits), Network Forensics, Crisis Management/Public Relations, Social Engineering, Bricking, Bodily Injury/Property Damage
Cyber Crime

- Fraudulent funds transfer vs. invoice manipulation & phishing
- Authentication challenges and risk management practices
- Other insurance clauses
- The Crime vs. Cyber debate
E&O and Cyber:
What is covered, which coverages respond and what triggers the coverage in your industry

<table>
<thead>
<tr>
<th>Errors &amp; Omission</th>
<th>Media</th>
<th>Network Security</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Third Party</strong></td>
<td><strong>Third Party</strong></td>
<td><strong>First Party</strong></td>
<td><strong>First Party</strong></td>
</tr>
<tr>
<td>• Negligence or Errors in the product of performance of services</td>
<td>• Infringement of intellectual property</td>
<td>• Unauthorized Access</td>
<td>• By Hacker</td>
</tr>
<tr>
<td>• Failure to perform</td>
<td>• Advertising &amp; Personal Injury</td>
<td>• Transmission of Virus or Malicious Code</td>
<td>• Lost data storably device</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Theft of data</td>
<td>• Bad Employee</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cyber Extortion</td>
<td>• Loss of Physical records</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Business Interruption</td>
<td></td>
</tr>
</tbody>
</table>
E&O and Cyber:

Financial loss coverage with Technology E&O

• Typically excluded from GL policies
• Claims arising out of the failure of the insured’s product to perform as promised, or an act, error, or omission committed by the insured in the course of its performance.
• Monetary loss caused by failure to deliver as promised or failure to meet contractual service levels & counter-argument

Exclusions regarding electronic data/access or disclosure of confidential information

• Bodily Injury carve-back and what it does
• BI/PD arising out of unauthorized access/technology failure to perform
Claim Example- Crime/Cyber

• **Type of claim:** Cyber
• **Cause of action:** Negligence/failure to perform
• **Type of insured:** Security Integrator – PSA Member

• **Situation:** Integrator had email compromised and hackers sent a falsified invoice and bank wiring instructions to a client of the integrator. Instructed to wire $500,000 which was done. The third party wired the money as instructed. Much of the money was recovered due to red flags noticed by the banks involved so the coverage for the full amount was not needed for the funds. The initial cost for forensics was $70,000.

• **Claim expenses:** $50,000 deductible to cover forensics cost. Remainder paid for under Cyber
Claim Example – E&O & Cyber

- **Type of claim:** Introduction of malicious code
- **Cause of action:** Failure to prevent introduction of malicious code
- **Type of insured:** Systems integrator

*Situation:* When uploading a new software program/integrating with hardware for a customer, a malicious code is inadvertently transferred to the customer’s network, causing widespread loss of data and disruption to the customer’s operations. In the download process, the virus spreads to the client’s computer system, resulting in widespread loss of data and a computer network shutdown. Challenge: The customer seeks damages for the costs to reconstruct the data, as well as the financial impact associated with the disruption of business operations.

- **Resolution Claim expenses:** $35,000 Indemnity: in excess of $400,000
Claim Example – Tech E&O

- **Type of claim**: Tech E&O
- **Cause of action**: Negligence/failure to perform
- **Type of insured**: Software/Hardware reseller
- **Situation**: A software/hardware reseller installs and provides maintenance services for accounting software applications that are specifically focused for retailers. A customer’s audit reveals that several journal entries were misclassified as a result of an error in the software program. While the problem is corrected, the customer incurs significant fees due to the misclassifications.
- **Challenge**: Customer sues the software reseller for damages associated with the additional work, including:
  - Audit fees
  - Costs to restate prior quarter financial statements
  - Accounting fees
  - Legal fees

**Resolution**

- **Claim expenses**: $35,000
- **Indemnity**: $120,000
Claim Example – Crime/Cyber

• **Type of claim:** Social Engineering
• **Cause of action:** Willful parting of funds
• **Type of insured:** Software/Hardware reseller

**Situation:** An employee received a call purporting to be from the company’s bank saying there had been a problem with a payment, possibly caused by a virus. The caller told the employee that the payment would have to be made manually and managed to extract some, but not all, of the bank security code. The employee became suspicious and alerted managers who immediately informed the bank. The bank put a stop on the account but not before eight transactions had been made.

• Social Engineering that results in fraudulent payments is more appropriately addressed in a crime policy as opposed to a cyber policy, but not always depending on the circumstances. The resultant forensic costs could be covered on a cyber policy.

• **Total Cost:** $520,000 less retention
Incident Response Plans and Risk Transfer

- Vendor risk management
- Familiarizing yourself with your legal counsel that comes with your Cyber policy
- The importance of involving all members of the board in Cyber Security decisions
- Keeping employee awareness and training standards high
- Encouraging reporting of incidents
- Limiting sensitive data privilege and requiring authentication
- Knowing where your most sensitive data is and limiting aggregation
- Keeping up-to-date with state and international privacy laws
- Limiting adverse media and any negative public/customer perception
Questions?