Agenda

• Compliance Environment
• IT Security Best Practices and Insurance Impact
• Cyber Threat Trends
• Evolution of Cyber Insurance
• Cyber Risk Management
State Regulatory Environment

48 out of 50 States

- A vast majority of US states have consumer protection statutes that address the safeguarding on consumer data

Personally Identifiable Information (PII)

- Protected / “Sensitive” information is defined differently in each state but there are common characteristics.

Data Owner vs. Data Aggregator

- Transfer of data to a third party does not constitute a shift in responsibility

Data Breach Victim’s State Residency Governs

Regulatory Testing Grounds

- California, Illinois, Massachusetts, New York
# Federal, Foreign & Industry Regulatory Environment

## Foreign Regulations
- GDPR becomes effective May 2018
- Chinese Cybersecurity Law

## FTC
- Bureau of Consumer Protection
- Division of Privacy & Identity Protection

## Payment Card Industry (PCI)
- PCI-DSS
- Merchant Service Agreement

## Contractual Obligations
- NDA / Confidentiality
- Insurance Requirements
IT Security Best Practices and Insurance Impact
Best Practices

PCI-DSS / Regulatory Compliance
- Payment Card Industry Data Security Standards
- Federal Regulations
- State Laws

Cyber Security Readiness
- Network Assessments
- Remediation of Vulnerabilities

Treatment of Private / Confidential Information
- Policies, Access Controls, Security Measures
- Quantification of Record Count / Transactions
- Encryption – At Rest, In Transit, On Portable Media Devices

Breach Preparation
- Incident Response Plan
- Business Continuity Plan / Back-up Procedures

Vendor Management
- Contract Review
- Professional E&O / Cyber Insurance and Indemnification Agreement
Cyber Threat Trends
Claims and Threat Trends

Cyber Loss Events: Ransomware

* Data for 2015 and 2016 are preliminary
Claims and Threat Trends

Cyber Loss Events: Network/Website Disruption

* Data for 2015 and 2016 are preliminary
Evolution of Cyber Insurance
Other Policies
NON-CYBER POLICIES ARE ADDING DATA BREACH EXCLUSIONS

COMMERCIAL GENERAL LIABILITY
FORMS FILING GL-2013-ODBFR

Access Or Disclosure Of Confidential Or Personal Information Exclusions Introduced

About This Filing

This filing introduces mandatory and optional exclusionary endorsements, for use with General Liability Coverage Part, addressing the access to or disclosure of confidential or personal information.

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

EXCLUSION – ACCESS OR DISCLOSURE OF CONFIDENTIAL OR PERSONAL INFORMATION AND DATA-RELATED LIABILITY – WITH LIMITED BODILY INJURY EXCEPTION

COMMERCIAL GENERAL LIABILITY
CG 21 06 05 14

EXCLUSION – ACCESS OR DISCLOSURE OF CONFIDENTIAL OR PERSONAL INFORMATION AND DATA-RELATED LIABILITY – LIMITED BODILY INJURY EXCEPTION NOT INCLUDED

COMMERCIAL GENERAL LIABILITY
CG 21 07 05 14
# Cyber and Other Policies

## Coverage & Gaps

<table>
<thead>
<tr>
<th>1st Party Privacy / Network Risks</th>
<th>Property</th>
<th>General Liability</th>
<th>Crime / Bond</th>
<th>K&amp;R</th>
<th>E&amp;O</th>
<th>Cyber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical damage to Data only</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virus / Hacker damage to Data only</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denial of service attack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B.I. Loss from security event</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extortion or threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee sabotage of Data only</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3rd Party Privacy / Network Risks</th>
<th>Property</th>
<th>General Liability</th>
<th>Crime / Bond</th>
<th>K&amp;R</th>
<th>E&amp;O</th>
<th>Cyber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft / Disclosure of private info.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidential corporate info. breach</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology E&amp;O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Liability (electronic content)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy breach expense / notification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Damage to 3rd party's Data only</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory privacy defense / fines</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virus / Malicious code transmission</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Coverage Provided?**
- Yes
- No Coverage?

*For reference and discussion only; policy language and facts of claim will require further analysis*
# 3rd Party Liability Coverages

## Network Security
- Failures in computer security
- Transmission of malicious software / viruses
- DDoS Attacks

## Privacy Liability
- Unauthorized Access or Use
- Failure to protect sensitive information

## Media Liability
- Online Content / Multimedia
- Libel / Slander / Defamation
- Copyright infringement

## Regulatory Defense, Fines & Penalties
- Regulatory Proceedings & Investigations
- Fines and Penalties where insurable by law

## PCI Defense, Fines & Penalties
- Defense Costs
- Fraud Assessments
First Party Coverage

- Cyber Extortion
- Digital Asset Restoration
- Business Interruption & Extra Expense
- Cyber Crime
- Breach Response Services
Cyber Risk Management: Incident Response Planning & Vendor Management
Cyber Incident Response Preparation

Incident Response Plan & Provider Identification

- Successful creation and implementation of an Incident Response Plan (IRP) is an extremely important step in cyber risk management
- An Incident Response Plan is essential for guiding you through a breach at the time of a crisis event

- Complete an IRP that includes your chosen providers
- Complete a Table Top Workshop to test your IRP
- Pre-negotiate service agreements with breach response providers
- Seek insurance carrier approval for chosen providers

Business Continuity Plan/Back-up Procedures

- Preparation is essential to minimize disruption of networks and continue operations without unnecessary delay.
- A thought out response may protect your organization's image, brand, and reputation

- Create and rehearse your business continuity
Cyber Incident Response

LIFE CYCLE OF A CYBER INCIDENT

- Insured becomes aware of incident
- Receive immediate advice and triage
- Notify your 24/7 Breach Response Counsel and contact your broker
- Notify insurance carrier
- Establish next steps
- Breach response:
  - Investigate incident
  - Prepare legal response and communications
  - Provide required notification and credit/ID monitoring
- Close incident
Vendor Management
UNDERSTANDING YOUR VENDOR RELATIONSHIPS

Contract Review & Professional E&O / Cyber Insurance Requirements

✓ Proper indemnification from your vendors will help to mitigate your vicarious liability should your chosen partner make an error that is out of your control
✓ Vendor Acceptance Process is vital

☐ Develop Errors & Omissions, Cyber, and Crime Insurance Contract Language designed to be made part of your existing insurance contract requirements
☐ *Develop reasonable requirements* that are relevant to the current cyber risk environment
☐ Prepare a vendor evaluation worksheet!!!
Vendor Management

SAMPLE CONTRACT WORDING – CYBER, E&O AND CRIME

Vendor) shall obtain at its own expense and evidence via Certificate(s) of Insurance the following insurance requirements before commencement of any awarded work and throughout the duration of the Agreement:

A) Errors and Omissions (E&O), Technology E&O / Technology Products E&O: minimum of $5 million limit and in the annual aggregate, inclusive of defense costs

B) Network Security / Privacy Liability; including
   (1) computer or network systems attacks
   (2) denial or loss of service
   (3) introduction, implantation, or spread of malicious software code
   (4) unauthorized Access and Use of computer systems
   (5) privacy liability
   (6) breach response coverage

   • Liability coverages should have a minimum of $5 million limit and in the annual aggregate
   • Breach response sublimits of at least 50% of the liability limit

C) Crime Insurance: Vendor, at its sole cost and expense, shall obtain and maintain in full force and effect, Third Party Crime/Employee Dishonesty Insurance in an amount not less than $1,000,000. The insurance shall name _____________ as a loss payee.

   If policy or policies are written on a claims-made basis, coverage must be in place for a period of at least 12 months after the completion or termination of the Agreement. "INSURED" and subsidiaries must be named as an additional insured under E&O, Technology E&O / Technology Products E&O and Network Security / Privacy Liability coverage sections. Further, an appropriate endorsement deleting the Insured vs. Insured exclusion must be evidenced, so as not to impede a claim by "INSURED" and subsidiaries for a wrongful act of (Vendor). All insurance carrier(s) must carry an A.M. Best rating of at least A-, Class VIII.
Thank You

Jeremy Gillespie
VP, Cyber Liability Practice
Arthur J. Gallagher & Co.
312-803-7394
Jeremy_Gillespie@ajg.com

Myles Miller
Underwriter
Beazley Group
312-476-6268
Myles.Miller@Beazley.com

Cuyler Robinson
VP, Forensic Services
Charles River Associates
312-619-3394
Crobinson@crai.com

Bruce Radke
Shareholder
Vedder Price
312-609-7689
Bradke@vedderprice.com