

### CYBER LIABILITY AND AVIATION



Presented by  
Hal Hunt  
May 3, 2015



ATA CONFERENCE  
2015

---

---

---

---

---



---

---

---

### AGENDA

- Introduction
- Learning Objectives
- Threat
- Examples
- Underwriting
- Protection/Cyber Policy
- Summary



ATA CONFERENCE  
2015

---

---

---

---

---



---

---

---

### LEARNING OBJECTIVES

- Understand Key Terms
- Understand The Threat
- Know The Right Questions To Ask
- Protect The Insured



ATA CONFERENCE  
2015

---

---

---

---

---

---

---

---

### KEY TERMS

- Breach - (FL Statute 501.171)
- Cyberattack
- Cyber Liability
- Cyberrisk



---

---

---

---

---

---

---

---

### THREATS TO CYBERSECURITY



---

---

---

---

---


---

---


---

### INTERNAL THREATS

- Weak Defenses
  - Cloud computing – Phones, tablets, self-service portals
  - Shared services
- Poor Use of Security Measures
  - Poor training
  - Weak discipline
  - Associated costs (IBM study estimates average cost of cybersecurity per employee is \$2500).



*The vast majority of hacking attacks are successful because employees click on links in tainted emails, companies fail to apply available patches to known software flaws, or technicians do not configure systems properly. Business Insurance 4-14-2015*



---

---

---

---

---

---

---

---

### THREAT CONTINUED

- 2013
  - 3000 small to midsize U.S. businesses hacked
  - \$1.2B spent on cyber insurance
- 2014
  - 783 breaches in 2014 (27.5% increase)
  - 85.6 million compromised records
  - 50% have less than 250 employees
  - \$2B spent on cyber insurance
- 2015
  - 1<sup>st</sup> Quarter already surpassed 2014



---

---

---

---

---


---

---


---

### DATA BREACH AND RELATED COSTS

- Average cost per compromised record – Overall = \$201.00
- Direct
  - Coordination – Legal, IT forensics, PR
  - Defense
  - Notification expenses
  - Credit monitoring
  - Regulatory fines – (46 states have regulatory requirements)
- Indirect
  - Customer churn
  - Time, effort, employee costs
  - Impact on shareholder value
  - Loss of future opportunity



Source: Ponemon Institute 2014 Annual Study "Cost of a Data Breach"



---

---

---

---

---



---

---

---

### POST BREACH EXPERIENCE

- Reputation management is the top concern
- 2014 Study Commissioned By IBM
  - 30% of customers are lost after a breach
  - 70% will not come back after a second
- 2015 1<sup>st</sup> Quarter Experian Industry Forecast
  - Average Breach Costs - \$3.5M
  - Surge in the adoption of Cyber Ins
  - Increased Cloud = Increased Breaches



---

---

---

---

---

---

---

---

### RECENT EXAMPLES

10

---

---

---

---

---

---

---

---

### WHERE IS THE GAP

	General Liability	Property	Crime	Professional	K&R	Cyber
1st Party Privacy/Network						
2nd/3rd Party Personal Liability						
Theft/Unauthorized Disclosure PI						
Breach of Confidential Corporate Info						
Technology Risk						
Media Liability/Social Networking						
Regulatory Defense/Penalties						
Virus/Malicious Code Transmission						
1st Party Privacy / Network Risks						
Legal Assistance/Breach Coach						
IT Forensics						
Physical Damage to Data						
Denial of Service Attack						
Business Income from Security Event						
Extortion or Threat						
Wage Employees - Data Related						
Public Relations/Crisis Management						
Coverage "Included"						
Coverage "Excluded"						

\*For reference and discussion only; policy language and facts of claim will require further analysis. This is not a guarantee of coverage.

---

---

---

---

---

---

---

---

### CYBERLIABILITY INSURANCE

**Third Party Coverage (Liability):**

- Network Security Liability
- Media/Website Liability
- Regulatory Liability

**First Party Response Coverage:**

- Crisis Management
- Security Breach Remediation and Notification
- Restoration Expenses
- Computer Fraud
- Fund Transfer Fraud
- Business Interruption
- E-Commerce Extortion

---

---

---

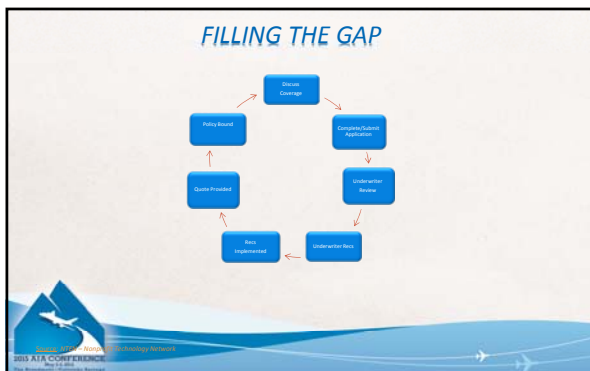
---

---

---

---

---




---

---

---

---


---

---

---


---

### QUESTIONS FOR YOUR INSURED




**Collection**

- What employee, customer, data are you storing?
- Do you need to store it?



**Access**

- Who in your business has access to sensitive information?
- Do those with access absolutely need access to perform their job?
- Where is your data stored?
- Is the stored information protected by access controls?
- Does sensitive customer information exist in multiple formats?
- Is the data accessible to third parties?
- Are your laptops encrypted?



**Eradication**

- How long do you keep customer information?
- What do you do with info (in any format) you no longer need?
- 3<sup>rd</sup> party vendor agreements for document storage, disposal, etc.

---

---

---

---

---

---


---

---

### HOW IS CYBERLIABILITY UNDERWRITTEN

BASED ON PERCEIVED RISK

- Controls in Place
- Types of Data Held
- Client Base
- Vendor Contract Management



Controls that will help:

- Firewalls/Antivirus
- Intrusion Detection
- Encryption
- Customer Notification Plan
- Internal Monitoring
- Risk Transfer

---

---

---

---

---

---

---

---



### APPLICATION PROCESS

Indication (2) questions

1. Name of Company
2. Total Revenue

Quote and bind (4) Questions

1. Total Revenue
2. Do you have anti-virus software installed and enabled on all desktops and servers (excluding database servers) and is it updated on a regular basis?
3. Do you also have firewalls installed on all external gateways?
4. Do you take regular back-ups (at least weekly) of all critical data?


---

---

---

---

---

---

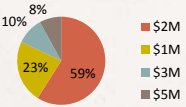
---

---

### BENCHMARKING & GUIDANCE


Revenue	Medium Limits Purchased
<\$50M	\$8M
\$50M - \$250M	\$25M
\$250M - \$500M	\$45M
>\$500M	\$58M

Liability Limits \$15M Company



- \$2M
- \$1M
- \$3M
- \$5M

*TechAssure 2015*




---

---

---

---

---

---

---

---

### CYBER POLICY OVERVIEW

**Travelers CyberRisk Policy**

- I. Insuring Agreements
- II. Definitions
- III. Exclusions
- IV. Conditions Applicable First Party
- V. Conditions Applicable Third Party





---

---

---

---

---

---

---

---

### EXCLUSIONS

A. Exclusions Applicable To All Insuring Agreements



- Nuclear, war, tangible property, emotional distress, mildew, fungus, etc.

B. Exclusions Applicable to First Party Agreements

- Pollution, prior knowledge, before inception, intentional acts, fraud, violation of the law,

C. Exclusions Applicable to Third Party Agreements

- Intentional acts, fraud, violation of the law, false or unfair trade practices, insured caused failure, etc.



803 ATA CONFERENCE  
By Appointment to the Governor of South Carolina

---

---

---

---


---

---


---

---


### SUMMARY



- Understand Key Terms
- Understand The Threat
- Know The Questions To Ask
- Protect The Insured



### QUESTIONS?



803 ATA CONFERENCE  
By Appointment to the Governor of South Carolina

---

---

---

---

---

---

---

---