Cyber Liability / Data Privacy Overview Discussion Points
Discussion Points

- Cyber Liability Overview
- What Constitutes Cyber Liability?
- Legislation and Privacy Regulations
- Data Breach Examples
- Is Southwire at Risk?
- How Do We Determine the Cost of a Breach?
- Insurance Due Diligence
- Summary
Cyber Liability Overview

**Issue:** Companies leveraging their business with computer networks or storing data face a breach risk resulting in the loss of sensitive data. That loss can adversely impact you and your customers, regardless of whether data was lost or stolen. The costs incurred to rectify the situation and comply with Federal/State laws and industry standard notification obligations will increase your company’s cost of doing business.

Traditional commercial insurances (i.e. CGL, property and crime policies) provide inadequate solutions to the unique challenges associated with data breaches. Those policies only apply to tangible assets and/or physical injuries. Losses resulting from data breaches, processes and network breaches may not be covered.
What Constitutes Cyber Liability?

- **Privacy liability** is the legal right to, or public expectation of privacy in the collection, use, disclosure, compilation or transfer of non-public information about individuals. The key exposures relate to financial and health information (codified in the privacy rules of **Gramm - Leach - Bliley Act of 1999** (G-L-B) and state laws).

- **Network security liability** relates to protection of sensitive or confidential electronic information from unauthorized access or use, which includes disclosure, theft of data, identity theft, etc. Refer to the security rules of **governmental regulations, numerous international and U.S. state laws**.
Legislation & Privacy Regulations

**United States**
- **US PATRIOT** (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act
- **Gramm-Leach-Bliley Act** (GLBA)
- **Health Insurance Portability and Accountability Act of 1996** (HIPAA) (Title II)
- **California’s Senate Bill 1386** (SB1386)
- **Sarbanes-Oxley Act** (SOX)
- **Fair and Accurate Credit Transaction Act of 2003** (FACTA)

**Non – US**
- **Personal Information Protection and Electronic Documents Act** (PIPEDA) (Canada)
- **European Union Data Protection Directive** (EUDPD)
- **Japan’s Personal Information Protection Act**
Legislation & Privacy Regulations

State Security Breach Laws
Fifty US jurisdictions, including 46 states, the District of Columbia, Guam, Puerto Rico, and the US Virgin Islands, have enacted notification laws.

Depending on state laws involved, it maybe the laws of the state where the effected individual resides that applies and thus not necessarily only the state where the breach occurred.

<table>
<thead>
<tr>
<th>Alabama</th>
<th>Louisiana</th>
<th>Oklahoma</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alaska</td>
<td>Maine</td>
<td>Oregon</td>
</tr>
<tr>
<td>Arizona</td>
<td>Maryland</td>
<td>Pennsylvania</td>
</tr>
<tr>
<td>Arkansas</td>
<td>Massachusetts</td>
<td>Puerto Rico</td>
</tr>
<tr>
<td>California</td>
<td>Michigan</td>
<td>Rhode Island</td>
</tr>
<tr>
<td>Colorado</td>
<td>Minnesota</td>
<td>South Carolina</td>
</tr>
<tr>
<td>Connecticut</td>
<td>Mississippi *</td>
<td>South Dakota</td>
</tr>
<tr>
<td>Delaware</td>
<td>Missouri</td>
<td>Tennessee</td>
</tr>
<tr>
<td>Dist. of Columbia</td>
<td>Montana</td>
<td>Texas</td>
</tr>
<tr>
<td>Florida</td>
<td>Nebraska</td>
<td>Utah</td>
</tr>
<tr>
<td>Georgia</td>
<td>Nevada</td>
<td>Vermont</td>
</tr>
<tr>
<td>Hawaii</td>
<td>New Hampshire</td>
<td>Virginia</td>
</tr>
<tr>
<td>Idaho</td>
<td>New Jersey</td>
<td>Virgin Islands</td>
</tr>
<tr>
<td>Illinois</td>
<td>New Mexico</td>
<td>Washington</td>
</tr>
<tr>
<td>Indiana</td>
<td>New York</td>
<td>West Virginia</td>
</tr>
<tr>
<td>Iowa</td>
<td>North Carolina</td>
<td>Wisconsin</td>
</tr>
<tr>
<td>Kansas</td>
<td>North Dakota</td>
<td>Wyoming</td>
</tr>
<tr>
<td>Kentucky</td>
<td>Ohio</td>
<td></td>
</tr>
</tbody>
</table>

Law is pending
No laws at present
* Mississippi law took effect 7/1/2011

(source Edwards Angell Palmer, & Dodge LLP)
Pending Legislation & Privacy Regulations


This is just a short list of the current 14 bills at the federal level that deal with privacy issues.

(source Covington & Burling LLP)
# Large Data Breach Examples

<table>
<thead>
<tr>
<th>Company</th>
<th>Type of Loss</th>
<th># of Affected customers/employees</th>
<th>Date of Initial Disclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Epsilon</td>
<td>Hacker</td>
<td>TBD</td>
<td>April 2011</td>
</tr>
<tr>
<td>TJ Maxx</td>
<td>Hacker</td>
<td>100 Million</td>
<td>January 2007</td>
</tr>
<tr>
<td>Card Systems</td>
<td>Hacker</td>
<td>40 Million</td>
<td>June 2005</td>
</tr>
<tr>
<td>Veterans Affairs</td>
<td>Lost Information</td>
<td>26.5 Million</td>
<td>May 2006</td>
</tr>
<tr>
<td>WorldPress</td>
<td>Hacker</td>
<td>18 Million</td>
<td>April 2011</td>
</tr>
<tr>
<td>Ibill</td>
<td>Employee Theft</td>
<td>17.5 Million</td>
<td>March 2006</td>
</tr>
<tr>
<td>Countrywide Financial</td>
<td>Employee Dishonesty</td>
<td>17 Million</td>
<td>August 2008</td>
</tr>
<tr>
<td>DeviantART, Silverpop Systems</td>
<td>Hacker</td>
<td>13 Million</td>
<td>December 2010</td>
</tr>
<tr>
<td>Bank of New York Mellon</td>
<td>Lost Computer Files</td>
<td>12.5 Million</td>
<td>March 2008</td>
</tr>
<tr>
<td>Fidelity National Information Services</td>
<td>Stolen Records</td>
<td>8.5 Million</td>
<td>July 2007</td>
</tr>
<tr>
<td>Hannaford Bros. Supermarket</td>
<td>Hackers</td>
<td>4.2 Million</td>
<td>March 2008</td>
</tr>
<tr>
<td>Citigroup</td>
<td>Lost or Stolen Info</td>
<td>3.9 Million</td>
<td>June 2005</td>
</tr>
<tr>
<td>Educational Credit Management Corp.</td>
<td>Data Stolen from Safe</td>
<td>3.3 Million</td>
<td>March 2010</td>
</tr>
<tr>
<td>Circuit City</td>
<td>Misplaced Information</td>
<td>2.6 Million</td>
<td>September 2006</td>
</tr>
<tr>
<td>J.P. Morgan Chase</td>
<td>Lost information</td>
<td>2.6 Million</td>
<td>September 2006</td>
</tr>
<tr>
<td>University of Utah Hospitals</td>
<td>Computer Theft</td>
<td>2.2 Million</td>
<td>April 2008</td>
</tr>
<tr>
<td>University of Miami</td>
<td>Computer Theft</td>
<td>2.1 Million</td>
<td>March 2008</td>
</tr>
<tr>
<td>Fox News</td>
<td>Hacker</td>
<td>1.5 Million</td>
<td>July 2007</td>
</tr>
<tr>
<td>DSW</td>
<td>Lost or Stolen Info</td>
<td>1.35 Million</td>
<td>March 2005</td>
</tr>
<tr>
<td>Gawker</td>
<td>Hacker</td>
<td>1.3 Million</td>
<td>December 2010</td>
</tr>
<tr>
<td>Avmed Health Plans</td>
<td>Computer Theft</td>
<td>1.2 Million</td>
<td>February 2010</td>
</tr>
<tr>
<td>Bank of America</td>
<td>Lost Information</td>
<td>1.2 Million</td>
<td>Feb. 2005</td>
</tr>
<tr>
<td>Blue Cross Blue Shield</td>
<td>Computer Theft</td>
<td>1.02 Million</td>
<td>Jan 2010</td>
</tr>
</tbody>
</table>
## Are you at Risk?

### Targeted Industries:
- Pharmaceuticals
- Healthcare
- Research/Education
- Service providers
- Financial Institutions
- Utilities/Energy
- Hotels/Leisure/Gaming
- Retail

### Data/Network Security Breach Triggers:
- Malicious/criminal attack (e.g. hackers, malicious employees, etc.)
- 3rd party (including employees) mistakes/negligence
- Theft/disappearance of private property (e.g. stolen laptop computer or other storage media)
- Systems malfunction/data corruption and damage
- Business interruption from own or key vendors system outages
- Data extortion

### Risk Assessment: Technology alone can not protect data. Companies need to implement best practices that address the following:
- **Data** – What sensitive data is stored? Where? Duration? Disposal?
- **People** – Who can access what data?
- **Processes/Policies** – Are these clearly written and current regarding data sharing? Are they enforced?
- **Technology** – Do you use firewalls? Encryption?

### Data/Network Security Litigation Sources:
- **Class action suits** – victims seeking damages (i.e. liability), remedial costs, time/value lost
- **Banks** – seeking damages, corrective costs, fraud expenses resulting from compromised data
- **Government** – FTC and/or State Attorney Generals
- **Other** – Industry standards (e.g. Payment Card Industry Data Security Standard, or “PCI DSS”)

Selected Recent Data Breach Examples
(Source: privacyrights.org)

July 7, 2011 Hurley Medical Center
A laptop was discovered missing in May. It was held in a locked room in Hurley, but it was not encrypted or password protected. The laptop contained the names, heights, weights, dates of birth, medical record numbers and lung function test results of 1,938 patients who visited Hurley between 2007 and May of 2011. A total of 10 out of 150 of Hurley's laptops were not encrypted at the time of the discovery.

April 21, 2011 ABM Industries
Televisions, mobile telephones and computers were stolen during a March 5, 2011 office burglary. One of the stolen computers contained tax reporting information, including Social Security numbers, for individuals employed by ABM in 2007 and 2008. One suspect was arrested sometime around March 22. The stolen computer was not recovered and ABM began notifying current and former employees of the breach on April 15.

April 4, 2011 Applied Micro Circuits Corporation
The February 23, 2011 theft of a laptop may have exposed the names and Social Security numbers of current and former employees. The laptop was stolen from an employee’s car. Those who were affected were sent notification on March 23.

January 6, 2011 Heraeus, Inc
A steel cabinet was discovered missing on November 18. The cabinet had a safe which contained IT data and software backup tapes. Personal information on the backup tapes included names, Social Security numbers, addresses, financial account numbers, driver's license numbers, medical information and other personal information. The cabinet was most likely thrown out during a cleaning. If so, the cabinet and its contents would have been taken to a transfer station, crushed, and then transported to a landfill for further destruction and disposal.
What are the Potential Risks?

Viable risks may endanger your operations:

- Loss of trade secrets and intellectual property
- Civil suits, individual and class action
- Regulatory enforcement actions
- Adverse publicity/reputation harm
- Suspension of business activity due to physical and non-physical (data) damages
How Do You Determine The Cost of a Breach?

Traditional View:
Dollars Per Compromised Record - $214 on average

Ponemon: 2010 Annual Study: U.S. Cost of a Data Breach
# Prepare / Prevent

## Steps

### Identify
- What information exists?
- Where is it?
- What format is it in?
- How easy or difficult is it to access?
- Are the systems and networks that hold the data secure?

## Challenges

### Comply
- Do you know what your regulatory and compliance requirements are?
- Are you meeting them?
- Are you familiar with international data privacy laws that impact your business?
- Do you have a records retention schedule and policy?
- Are you utilizing storage technologies that will support your compliance with regulatory requirements?

## Services

### Protect
- Do you have a response plan should a breach incident occur?
- Are you securely destroying data and storage that has met the end of its retention period or lifecycle?

### Data Mapping & Inventory
- Table Top Exercise
- Data Accessibility Assessment
- Data Security Assessment and Strategy
- Vulnerability Testing
- Credit Monitoring
- Network Monitoring

### Complying
- Records Retention Consulting
- Data Preservation and Collection
- Compliance and Global Data Privacy
- Data Archiving
- Incident Response

### Protecting
- Incident Response Strategy
# Respond/Remediate

## Steps

### Investigate
- Retain Outside Counsel with Privacy Law Expertise
- Determine the scope of the breach and potential notification duty
- Ensure that the breach has been contained
- Determine what or who caused the breach
- Document investigation and findings in a legally defensible manner

## Challenges

- Determine the scope of the breach and potential notification duty
- Ensure that the breach has been contained
- Determine what or who caused the breach
- Document investigation and findings in a legally defensible manner

## Services

### Respond
- Retain Crisis Management / Reputational Advisory
- Ensure potentially impacted parties are contacted in a timely and professional manner
- Provide a remediation resource for impacted parties

### Defend
- Regulatory Defense
- Civil Defense
- Recover from the breach with confidence, knowing your legal matters are being expertly handled
- Ensure that your systems and data are protected from future breaches or attacks

### Incident Response
- Data Preservation and Collection
- Breach Scope Determination
- Information Security Consulting
- Network and Forensic Data Analysis
- Breach Investigation
- Business Investigation Services
- Custodian Interviews

### Breach Notification
- Breach Contact Call Center Support
- Identity Theft Investigation and Restoration
- Credit Report and Non-Credit Searches
- Continuous Credit Monitoring

### Expert Testimony
- Information Technology
- Remediation
How Cyber Liability Responds (If Purchased)

BREACH OCCURS:

1. Notify Insurer of data/privacy breach.

2. Breach attorney and forensic expert investigate, advise and report on scope of breach and application of notification laws.

3. Insured, legal counsel and insurer determine notification requirements. Notification service provider selected to comply with requirements.

4. Selected credit bureau (with the assistance of the insured and counsel) prepares script for call center employees.

5. Notification service provider sends letters post insured/attorney approval.

6. Call center field inquiries from notified individuals.

7. Individuals decide on credit monitoring package.

8. Insured receives progress reports of the mailing and credit monitoring enrollment.
Summary

- Convergence of exposures
- Threat and damages are real
- Cyber risks represent significant civil liability and regulatory exposure
- It’s a board room issue and your network is a critical asset
- Many insureds (incorrectly) believe coverage exists under traditional policies
- Technology solutions alone can’t eliminate network risk
Robert G. O’Shea, Jr.
Managing Director
Beecher Carlson

Bob O’Shea brings to Beecher Carlson more than 30 years of experience in the insurance industry. Prior to joining Beecher, Bob was a Senior Casualty Account Executive in the Marsh Stamford, Connecticut office after serving as a Casualty Department Team Manager in New York. After returning to New York, Bob was appointed as the Errors & Omissions Risk Practice leader for Marsh FINPRO, New York in 2004.

In his current role at Beecher Carlson, Bob is responsible for designing, negotiating and delivering Executive Liability’s products including Directors & Officers Liability, Professional Liability, Employment Practices Liability, Fiduciary Liability, Crime and other related Executive Liability insurance lines and works extensively on Fortune 1000 and complex risks, nationally.

Bob holds an A. A. S. Degree in Accounting from Suffolk Community College and a B. A. in Economics from the State University College of New York at Oneonta.